The STEPS Quality Manual

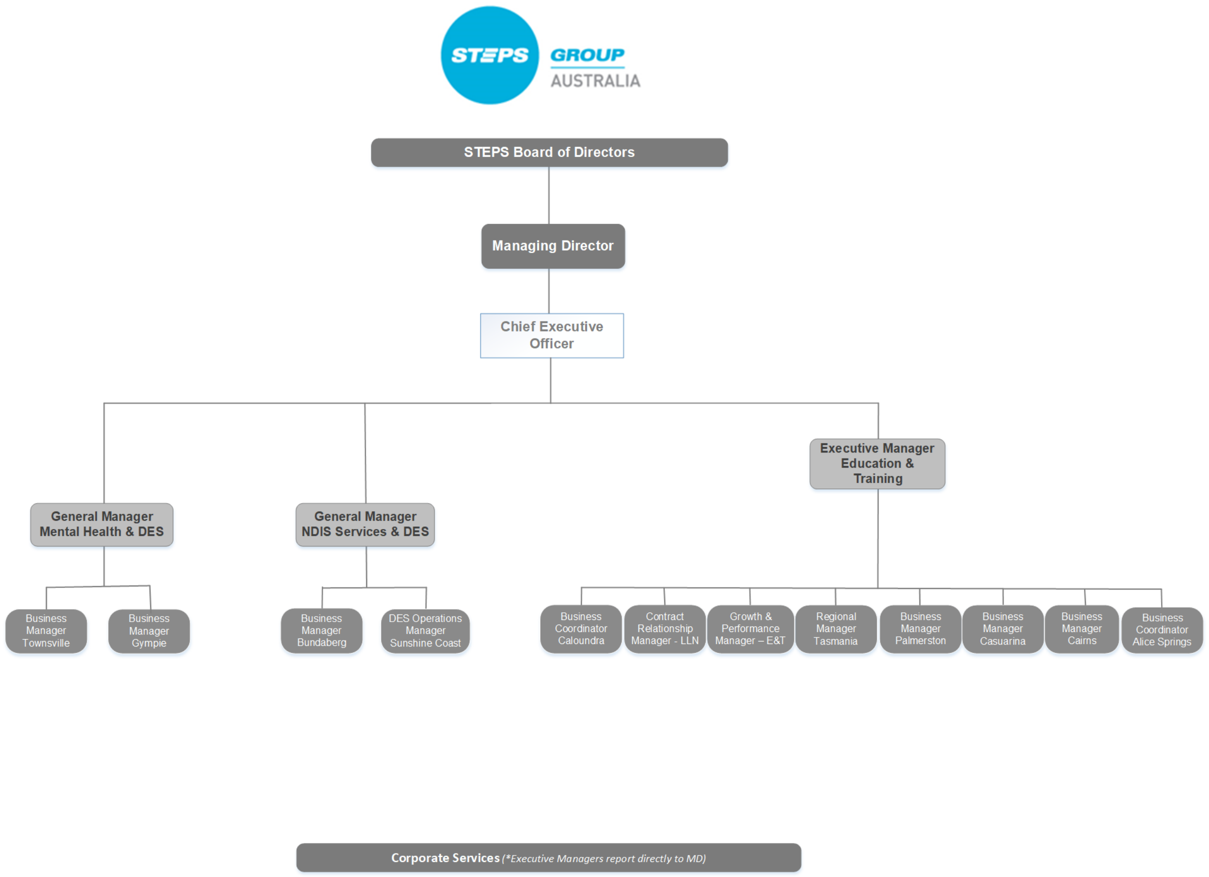
USER MANUAL

STEPS Disability Qld Inc.

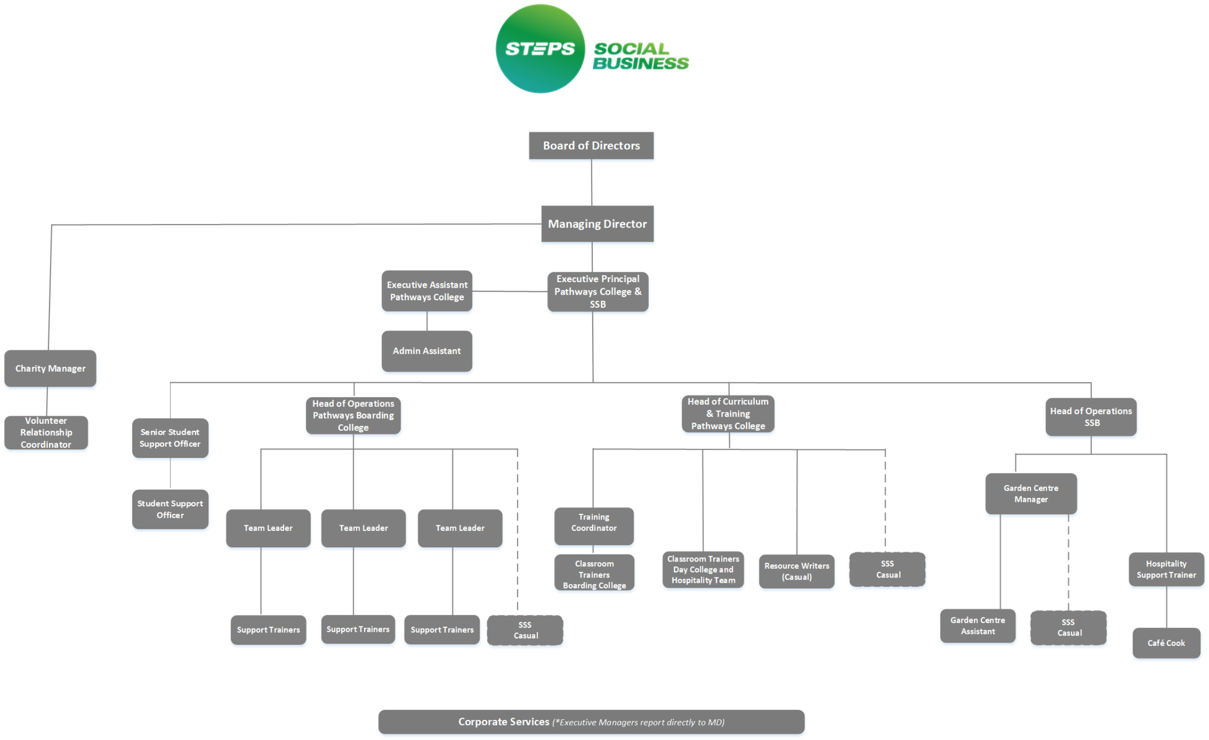
STEPS Organisational Policies & Procedures

1 STEPS Organisational Policies & Procedures

STEPS Group Australia - Organisation Chart (i010205)


STEPS GROUP AUSTRALIA
STEPS Board of Directors
Managing Director
Chief Executive Officer
General Manager Mental Health & DES
General Manager NDIS Services & DES
Executive Manager Education & Training
Business Manager Townsville
Business Manager Gympie
Business Manager Bundaberg
DES Operations Manager Sunshine Coast
Business Coordinator Caloundra
Contract Relationship Manager - LLN
Growth & Performance Manager – E&T
Regional Manager Tasmania
Business Manager Palmerston
Business Manager Casuarina
Business Manager Cairns
Business Coordinator Alice Springs
Corporate Services (*Executive Managers report directly to MD)

STEPS Staffing Solutions - Organisation Chart (i010204)


STEPS SOCIAL BUSINESS
Board of Directors
Managing Director
Executive Assistant Pathways College
Executive Principal Pathways College & SSB
Admin Assistant
Charity Manager
Volunteer Relationship Coordinator
Senior Student Support Officer
Student Support Officer
Head of Operations Pathways Boarding College
Team Leader
Team Leader
Team Leader
Support Trainers
Support Trainers
Support Trainers
SSS Casual
Head of Curriculum & Training Pathways College
Training Coordinator
Classroom Trainers Boarding College
Classroom Trainers Day College and Hospitality Team
Resource Writers (Casual)
SSS Casual
Head of Operations SSB
Garden Centre Manager
Garden Centre Assistant
SSS Casual
Hospitality Support Trainer
Café Cook
Corporate Services (*Executive Managers report directly to MD)

i010204_v1_241010

1.1 STEPS Quality Manual

STEPS Quality Manual
STEPS Organisational Policies & Procedures
STEPS EMPLOYMENT SOLUTIONS
STEPS EDUCATION & TRAINING
STEPS SOCIAL BUSINESS
STEPS COMMUNITY SUPPORT
Mental Health Programs
STEPS Autism Treehouse
STEPS PATHWAYS CHARITY
ndis
REFERENCE
Reference Documents & Standards
STEPS Values & Commitment

1.2 Governance and Policies

Our Commitment

To make a difference by providing opportunity

Our Values

Integrity - Our actions match our words.

Courage - Together we have the courage to find innovative solutions.

Respect - We treat everyone equally and fairly.

Understanding - We prioritise understanding the needs of our customers and our community.

1.2.1 Anti-Discrimination and Equal Employment Opportunity Policy

STEPS Group of Companies (STEPS) is a not-for-profit organisation committed to *making a difference by providing opportunity*.

STEPS values diversity and seeks to create an inclusive environment that accepts each individual's differences, embraces their strengths and provides opportunities for everyone to contribute their unique experiences. This allows each person to impact positively on the organisation ensuring that its services are delivered in a manner that respects and values the customs, cultures and beliefs of its customers and workers.

STEPS recognises its obligations under the legislation in relation to discrimination. This legislation includes: Australian Human Rights Commission Act 1986; Age Discrimination Act 2004; Disability Discrimination Act 1992; Racial Discrimination Act 1975; Sex Discrimination Act 1984, Workplace Gender Equality Act 2012 and relevant state legislation. Discrimination on the following grounds is unlawful:

- Race.
- Age.
- Impairment.
- Religious belief or activity.
- Sex or gender identity.
- Relationship status.
- Sexuality.
- Pregnancy, breastfeeding, parental status.
- Family responsibilities.
- Lawful sexual activity as a sex worker.
- Trade union activity.
- Political belief or activity.
- Those subject to family and domestic violence.
- Association with someone else who is identified because of one of the above attributes.

Discrimination can be:

- Direct - when someone is dealt with unfairly on the basis of one of the grounds listed above (compared with someone who doesn't have that ground); or
- Indirect – when a policy, rule or practice seems fair because it applies to everyone equally, but, some people or groups of people, are unable or less able to comply with the rule or are disadvantaged because of it.

To succeed in creating an inclusive environment STEPS offers equal employment opportunities (EEO), which means people are treated on their merits at every stage of their employment experience.

To achieve an inclusive workplace, supervisors will ensure the implementation of this policy and:

1. Promote the benefits of having a diverse and inclusive work environment and participate in events that support and celebrate diversity.
2. Role model the use of non-discriminatory language, practices and EEO principles.
3. Hold all workers and customers accountable for their actions in complying with this policy.
4. Identify and address any breaches of this policy, following any supporting procedures.

5. Be aware of different cultural practices, customs and special needs and be prepared to make reasonable adjustments where appropriate.
6. Report any behaviour that may be discriminatory and work to resolve complaints and eliminate unlawful discrimination.

This Policy was ratified by the Board on 29 February 2024.

To access a print friendly version of this Policy please click here.

1.2.2 Artificial Intelligence (AI) Use Policy - Marketing and Communications

1.0 INTRODUCTION/GENERAL

Artificial intelligence (AI) refers to the ability of computer systems to perform tasks which normally require human intelligence such as understanding natural language, recognising patterns, making decisions, and solving complex problems. However, artificial intelligence tools cannot mirror the complexities of human reasoning especially when it comes to moral and ethical considerations.

Generative AI tools make predictions based on vast amounts of existing content rather than creating original work, and they cannot replace human creativity. These tools can help enhance productivity, but they will not replace the role of a human-centred approach at STEPS and its related entities.

This policy is to guide the use of generative AI and is not intended for functions relating to data analysis, research, chatbots etc

1.1 DEFINITIONS

Word	Definition
AI model	The algorithm used to interpret, assess, and respond to data sets based on the training it has received.
AI system	The infrastructure that uses the AI model to produce output based on interpretations and decisions made by the algorithm.
Approved AI	Microsoft Co-Pilot App
Deep Learning	This is a subset of machine learning that uses multi-layered neural networks to simulate the complex decision-making power of the human brain.

Generative AI

A type of AI that can generate a wide variety of data, such as images, videos, audio, text and 3D models.

Machine Learning

A type of AI and computer science that focusses on the use of data and algorithms to enable AI to imitate the way that humans learn, gradually improving its accuracy.

Personally identifiable information

A set of data that could be used to distinguish a specific individual. This may include an individual's name, signature, address, phone number or date of birth.

Public AI

An AI system that a vendor makes available to any user who wants access and that collects and uses their inputs to improve the algorithm's performance. Unlike private AI systems, public systems send data outside the organisation.

Private AI

A proprietary AI system developed and used by the organisation, keeping data within the company.

Responsible AI

A set of guiding principles to promote ethical use of AI.

Sensitive Information

This is a subset of personal information that requires greater protection under the Privacy Act. This information includes race or ethnic origin, political opinions, religious beliefs etc.

2.0 ACCEPTABLE USE OF AI

The AI-generated marketplace is dynamic, and it would be impossible to list all allowed and prohibited use cases. This information, along with the Guiding Principles below, is here to provide direction. This is a living document and may change as technology, legal review and other policies change.

STEPS strongly encourages employees to familiarise themselves with available generative AI tools. Practice using them to see how they can help enhance productivity in your role.

Employees may use Gen AI for approved business processes such as resume content and communications, provided those organisational standards to protect data confidentiality and integrity, as laid out in this policy and elsewhere, are upheld.

- Employees are not permitted to enter unapproved data types into public AI systems, and the use of personal identifiable information or sensitive data is strictly prohibited.

- Any exception to the use of sensitive data in public AI systems must be formally approved by the data owner before any action can occur. Where confidential information is to be used the employee will be provided with a Private AI account. The Managing Director/Chief Executive Officer can approve roles that require private AI accounts and it is expected that the people in the roles will have completed appropriate training or have necessary knowledge and skills to protect data confidentiality and integrity and who only use it as part of approved business processes.

Employee use of Gen AI systems must be lawful and not jeopardise the organisation’s professional reputation or brand.

Prior to use of Generative AI, employees must read the Complying with Australian Privacy Procedure and be familiar with the guiding principles for responsible AI use detailed below.

All suspected or confirmed cases of compromised data breaches must be reported in accordance with the data breach procedure.

2.1 ACCEPTABLE USE OF AI FOR MARKETING AND COMMUNICATIONS

The below information is for marketing and communications professionals who work for STEPS, and they are not intended for other areas of the organisation. They apply to AI tools used to generate content, such as images, text, music, video, and other similar items.

For the purposes of this document, content is meant in its broadest sense and refers to articles, press releases, feature stories, websites, web content, podcasts, videos, etc.

- **Brainstorming new story ideas:** AI can help with fresh story ideas, and it can offer a different perspective or provide constructive feedback on existing concepts for content.
- **Creating an outline:** AI can organise content ideas into a cohesive structure.
- **Editorial calendar/content plan:** AI can help you quickly organise and plan your content and social media calendars.
- **Helping with headers, headlines, and other content structure and navigation**: AI tools can help you identify common themes and provide draft ideas for headlines, subheads, website headers, H3 tags, etc.
- **Search engine optimisation (SEO):** AI tools in the marketing and communications realm can quickly assist with keyword research and help analyse factors like readability, keyword usage, and relevancy to improve webpage quality and performance, among other uses.
- **Helping draft social media posts:** AI tools can be a great place to start for a quick first draft of social media posts. They can also help you tailor existing social media posts, comments, etc. to different audiences and drive engagement.
- **Getting started with research:** Ask AI tools to quickly teach you about a concept or topic. From beach volleyball rules to scientific concepts, it can be an outstanding research assistant. However—as stated previously—humans must verify all facts, research, knowledge, and information. Keep in mind, AI tools can “hallucinate” and fabricate information.
- **Personalising messaging:** AI tools can be adept at helping you rework your content to reach different audiences, such as students and participants, donors, or the media. It can make suggestions for how to change language, shorten text, emphasise different targeted messages, etc.

- **Anticipating potential questions or objections:** Ask an AI tool to behave like an investigative journalist and suggest potential questions or objections from stakeholders so you can prepare responses in advance.
- **Serving as a thesaurus:** AI tools can help you replace a word or phrase or rework a section of content.
- **Enhancing productivity:** Provided privacy policies are followed, AI tools can help with routine tasks such as summarising interview transcripts, analysing data, drafting outlines and text for presentations, etc. AI may be able to help draft emails, but it is vital not to rely on AI alone.
- **Tightening a piece:** Paste content that's too long into an AI tool and ask it to identify areas you could cut. It will look for places of repetition or where shorter phrases would suffice. Note: these suggestions should still be reviewed by humans, especially since it may suggest changes to quotes or adjust factual information.
- **Improving an image**: Use of content-aware fill functionalities in photo editing software, such as Photoshop, Canva, etc. is permitted within these guidelines for images you already own. Content-aware fill is considered an assistive tool that can enhance productivity and improve the visual quality of marketing and communications materials by seamlessly retouching or removing unwanted elements from images. However, we emphasise that the primary purpose of photo editing tools in this context is to assist and augment human creativity rather than replace it. Additionally, it is crucial to ensure that the use of these tools does not fundamentally alter the context or integrity of the image, maintaining the image's authenticity and intended message.

To reiterate, AI tools are assistive, not autonomous. They are writing and content aids and cannot replace the role and importance of the human in these tasks. Additionally, these are examples of acceptable and prohibited use, not an exhaustive list.

3.0 GUIDING PRINCIPLES FOR RESPONSIBLE USE OF AI

STEPS believes in:

- a human-centred approach to AI that empowers and augments professionals. AI technologies should be assistive, not autonomous.
- in the critical role of human knowledge, experience, emotion, and imagination in creativity, and we seek to explore and promote emerging career paths and opportunities for creative professionals.
- the power of communication to educate, influence, and effect change, generative AI must never knowingly be used to deceive or spread misinformation

STEPS employees will be accountable for all decisions and actions, even when assisted by AI. All AI generated material must be carefully reviewed, approved, edited and overseen by a human author.

Employees using AI must verify the accuracy of information supplied by AI. Nothing can replace the role of human fact checkers, and we must take responsibility for any AI-assisted information used by STEPS.

STEPS recognises that AI generated materials have a high probability of capturing the copyrighted material of another person. Therefore, employees will need to take great care to assure that the final product of any AI generated material has been carefully reviewed, and where necessary modified, to avoid plagiarism.

In order to maintain the trust of our audiences and stakeholders STEPS believes that transparency in AI usage is essential and, therefore, AI should be acknowledged when used.

4.0 PROHIBITED USE OF AI

AI tools should not be used in any way that would violate existing business standards or policies. For example, creating false communication, spamming/phishing, or manipulating data to create a deceitful impression.

AI tools are not encrypted or private. Do not enter proprietary data, information about employees or other constituents that could be a breach of state or federal privacy laws, including the Privacy Act 1988, the Australian Privacy Principles (APPs), the Health Records Act, or other business policies.

Additionally, ensure compliance with industry-specific regulations such as the Notifiable Data Breaches (NDB) scheme. Information submitted to many AI tools has the potential to become public and part of the promptable knowledge base.

AI tools should not be used to create entire pieces of written content. It can be used for tasks such as brainstorming, drafting headlines, and targeting messaging. But fully AI-generated content is prohibited at this time.

Unfettered fact-checking is prohibited. AI tools are outstanding research assistants but may “hallucinate” and suggest facts and sources that are entirely inaccurate, though they sound plausible. Again, humans must be central to all research, content creation, and review.

Additionally, AI-generated images, music, audio, and video should not be used in STEPS’ communications materials. The legality of this practice is under review in the courts, and the ethics are dubious. Instead, AI can be used to help brainstorm art ideas and direction.

Some artists are pursuing legal recourse against organisations using AI-generated art rather than against the AI companies themselves. Real-world example: A large tech company recently shared an AI-generated image on its channels. An artist recognised his work prominently used in the piece and threatened a lawsuit unless the tech company compensated him. Companies that use AI-generated art are being advised to include indemnification clauses in contracts.

5.0 HOW TO USE AI IN 3 SIMPLE STEPS

When using generative AI such as Copilot you simply ask for what you need.

Action	Explain what you want Copilot to do.

Style	Describe the format you want in the response presented in.
Key details	Context about your situation.

For example:

- Please give me three novel recommendations for my book club.
- Give your answer in a table that includes the book title, summary and four discussion questions each.
- My club consists of millennials, aged 30 to 35. We are avid readers interested in mystery, drama and romantic novels. We meet in person weekly, so please give me a reading schedule corresponding to the meeting cadence.

https://news.microsoft.com/source/features/ai/how-to-use-ai-in-3-simple-steps-just-ask/

6.0 ACKNOWLEDGING THE USE OF AI TOOLS

If you use generative AI in the development of resources, pictures or documents you should acknowledge this by providing a description of the AI tool used, how the information was accessed and the date.

Example: I acknowledge the use of Microsoft Copilot to generate the pictures used in this PowerPoint presentation.

This Policy was ratified by the Board on 24 September 2024.

To access a print friendly version of this Policy please click here

i010118_v1_241002

1.2.3 Change Management Policy

STEPS Group of Companies (STEPS) is committed to *making a difference by providing opportunity*, which is often driven through the introduction of innovation and improvements in the way we deliver services and the types of services we provide.

These types of changes inevitably impact people, processes, and technology, it is important that these changes are supported, which may include physical assets, human resources, and marketing.

STEPS' quality management system is based on the principles of ISO 9001:2015 and complies with the requirements on ISO 27001:2022.

The purpose of this policy and the associated procedures is to provide a framework to enable STEPS to approach change in a coherent manner, to achieve the maximum benefits from change whilst minimising disruptions and negative, or unintended outcomes.

STEPS is likely to deal with several different types of change events. These could include but are not limited to:

- Changes in scale – where new tenders or grants are awarded, mergers occur, or new sites are opened.

- Changes in structure or staffing – from time-to-time it will be necessary to adjust staffing levels, organisational structure or key supervisory or management roles, all of which may impact team dynamics and team performance.
- Changes in technology – where information communications technology requires updating or equipment changes to provide the required level of reliability and security of the ICT infrastructure.
- Changes in service offerings – when new services are added or improvements in current operating processes are introduced existing employees may need training, additional employees may need to be recruited, new premises opened, or new equipment introduced.
- Regulatory and Compliance changes – shifts in laws, regulations or contracts can have significant impact on how work is undertaken.

STEPS Change Management framework contains procedures including:

- Change Management (i011200)
- Project Management (i010700)
- ICT Change Management (6002400).

The Change Management process will include:

- Identifying the need for change.
- Initiating a change request through various ticketing systems, change request, Innovation Idea or Project Proposal (i010713) forms which will include a reason for the change.
- A review of the change request for feasibility, desirability and priority.
- As assessment or evaluation of the change to understand consequences, effect on overall performance, impact on information security, risks.
- Resources will be identified to ensure the capacity and capability to make the change.
- Final approval for the change.
- Plan, execute and deliver the change though business as usual activities (BAU) such as team meetings or performance reviews, following the project lifecycle outline in the Project Management Framework (i010702) or through scheduled system updates.

This Policy was approved by the Chair on behalf of the Board on 11 July 2024.

To access a print friendly version of this Policy please click here.

1.2.4 Child and Youth Safety and Wellbeing Policy

STEPS Group of Companies (STEPS) is a not for profit organisation committed to *making a difference by providing opportunity*.

STEPS is committed to providing a service environment that protects children from harm and focusses on their safety and wellbeing in accordance with legislation, including the *Working with Children (Risk Management and Screening) Act 2000* (Qld); and the *Care and Protection of Children Act 2007* (NT).

The purpose of this policy and the associated procedures is to provide a framework for ensuring children and youth are protected and that all workers know how to mitigate the risks of harm to children and youth in our service environment and also, know what to do should they become aware of conduct that does not support this policy and commitment.

STEPS child and youth risk management framework contains policies and procedures including Recognising and Responding to Abuse, Neglect and Exploitation Procedure (i051400); Incident Notification (i090200); Code of Conduct and Ethical Behaviour (e210007); Recruitment and Selection (e200100); Criminal History Checks (e200200); Feedback and Complaints Policy (i010103); Feedback Procedure (i040100); Complaints Procedure (i040500); Risk Management (i050100) and Employee Grievance (e210100).

This policy is built on the following principles:

- Supporting procedures provide a seamless link between prevention, reporting, investigating and determining solutions for incidents or suspicion of abuse, neglect and exploitation.
- All workers delivering services to children and youth at STEPS will be required to hold a positive notice letter and the relevant card in accordance with state and commonwealth legislation (for example blue card, ochre card).
- Workers will receive information and training during their induction and throughout their employment on STEPS child and youth risk management strategy and the associated policies and procedures.
- Managers/supervisors and workers will undertake risk assessments when undertaking activities or special events involving children and young people to identify potential risks and develop and implement effective risk management plans to remove or minimise the risks of harm to children and young people.
- All reports of abuse, neglect and exploitation will be taken seriously and responded to promptly and confidentially.
- If abuse, neglect or exploitation is reported or suspected workers should respond:
  - Calmly and with sensitivity
  - Providing a safe and private environment
  - Explaining that the information will need to be reported
  - Limiting questions to facts (what, when, where, who), avoiding probing questions
- Workers must inform their managers/supervisors of any incidents or disclosures managers/supervisors will evaluate the risk and will consider the need for internal investigation or appropriate referral of the incident or disclosure, they will also determine reporting requirements to relevant Government services if the child or youth is receiving funding through the National Disability Insurance Scheme (NDIS) the NDIS Quality and Safeguarding Commission will need to be notified within 24 hours in accordance with the NDIS Incident Management and Reportable Incident Rules 2018.
- Workers will be supported during any part of the process and will be offered debriefing services or Employee Assistance.
- A worker in breach of this policy or a worker who makes a vexatious or malicious complaint will be managed through a disciplinary process which may include suspension from work if the worker is under investigation (internally or by the police) for committing abuse, neglect and exploitation through to terminating the employment of an employee and ceasing all involvement of a volunteer.

This Policy was ratified by the Board on 31 March 2023.

To access a print friendly version of this Policy please click here

1.2.5 Communication Policy

STEPS Group of Companies (STEPS) is committed to creating a workplace where all workers feel well-informed and engaged in the various activities, functions, events, and services provided by STEPS. The purpose of the policy is to outline how STEPS uses communication to assist the business run as effectively as possible to achieve the best outcomes for our colleagues, stakeholders, customers, participants, and students.

Workplace Communications occur at all levels of STEPS and will range from formal meetings, STEPS Intranet and kitchen or corridor conversations. At all times workers are to respect every other person in the organisation and others they come into contact within a business context. Treating everyone with courtesy, friendliness and in a spirit of helpfulness will benefit individuals and the organisation as a whole. Differences of opinion should be handled discreetly and privately communicating directly with the person involved to resolve differences. Workers should strive to always maintain a civil work atmosphere and refrain from shouting, yelling, using vulgarities or swearing. Any inappropriate remarks about others or groups of people that may be considered humiliating, intimidating, or threatening, victimising, or insulting will not be tolerated.

Electronic and Wireless Communication devices, such as mobile phones or tablets provided by STEPS are to be used by employees to ensure they are contactable during work hours, while travelling or other times as instructed. Using only company approved devices and email accounts assists in ensuring information security and allows separation and segregation of work-related information from personal information. Refer to the Information Security Management System (ISMS) for more detailed information in relation to the handling of information and use of ICT services and equipment.

Social media communication on behalf of STEPS is managed by the Marketing and Communications Team, workers are encouraged to like and share posts. It is important to note that any comments on personal social media platforms about the organisation or other workers is covered by Workplace Bullying and Harassment Policy (i010105) and the Code of Conduct and Ethical Behaviour (e210007) and the Social Media Procedure (e210200) and may be subject to disciplinary action if the communication is derogatory, defamatory, or harmful to STEPS' reputation.

Communicating change will be done as part of the Project Management Framework Summary (i010707) and the Change Management Procedure (i011200) with the aim of keeping all workers informed of changes, the reasons for the change and the benefits the change will deliver. All changes to ICT will be managed in accordance with the ICT Change Management Procedure (6002400) to ensure information security is maintained during upgrades to ICT infrastructure and services or changes to access and permissions.

Communicating externally about the business or an event impacting the business is only to be done by the Managing Director. If an employee receives a request from the media, they must refer the request to the Managing Director immediately. This is to ensure that consistent and accurate messaging is issued to the public and to ensure STEPS' reputation is upheld and avoid any serious financial or legal consequences.

Feedback from workers, customers, participants, and students is always welcome to assist STEPS to improve its services, the work environment and enhance the customer experience. All workers are encouraged to facilitate the recording and resolution of complaints using the Feedback Procedure (i040100) and Complaints Procedure (i040500). If employees have concerns about their experience in the workplace, they should refer to the processes in the Employee Grievance Procedure (e210100) and the Whistleblower Procedure (i090500).

Adopting the communication approaches in this policy will ensure all people are treated with respect and understanding. This will assist in creating a supportive and inclusive environment in which everyone, workers, customers, participants, and students alike, feel valued and informed with a strong sense of belonging.

This Policy was ratified by the Board on 30 May 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here

1.2.6 Conflict of Interest

1.0 INTRODUCTION

All employees of STEPS Group of Companies (STEPS) have obligations and responsibilities to act appropriately when a conflict of interest arises between self-interests and duties to STEPS, organisations and funding bodies with whom STEPS has dealings (e.g. Federal Government, Private Sector Businesses).

Where a conflict of interest may arise, the conflict should be managed in accordance with this procedure.

1.2 DEFINITIONS

Conflict of Interest	A conflict of interest can arise from gaining personal advantage, avoiding personal losses as well as financial or otherwise.
Actual Conflict of Interest	Involving a direct conflict between current duties and responsibilities and existing private interests.
Perceived Conflict of Interest	Conflict existing where it could be perceived, or appears, that private interests improperly influenced the performance of duties – whether or not this is in fact the case.
Potential Conflict of Interest	Arising where private interests could conflict with official duties.
Pecuniary	Involving financial gain or loss.
Non-Pecuniary	Based on feelings (either dislike or friendship).

2.0 DISCLOSURE OF CONFLICTS OF INTEREST

There is nothing unusual or necessarily wrong in having a conflict of interest, the important thing is how it is dealt with. Disclosure must be made in full to the relevant member of the Executive Leadership Team (ELT) using the Conflict of Interest Disclosure form (i010501).

An employee's primary obligation is to notify the relevant member of the ELT as soon as they are aware, or in advance of any conflict of interest, be it actual, perceived or potential. Such conflict of interest is then assessed and particularly for financial decisions, written approval should be obtained before any commitment is made that might involve an actual, perceived or potential conflict of interest.

Failing to disclose an actual, perceived or potential conflict of interest can be regarded as misconduct, including serious misconduct and the matter will be dealt with accordingly.

3.0 MANAGING CONFLICTS OF INTEREST

The ELT member will be responsible for conducting an assessment to determine if an actual, perceived or potential conflict of interest exists.

Where a conflict of interest is determined to exist, a management plan must be developed to resolve and manage the conflict of interest. This Management Plan is to be recorded on the Conflict of Interest Disclosure form (i010501) .

3.1 A MANAGEMENT PLAN

A management plan states matters including:

- The nature of the employee’s personal interests.
- The interest/s with which the employee’s personal interest, or business arrangements do, or could conflict.
- The likelihood of the interests actually coming into conflict.
- The decisions or actions which the employee agrees to avoid doing or participating in.
- Which, if any, management employees need to be aware of the management plan to facilitate its implementation.
- The decisions or actions which it is agreed the employee can take or do.

Once a management plan is devised, it must be:

- Signed by all parties and placed on the employee’s personnel file.

All documents should be marked “confidential” and access limited to those management employees identified in the management plan.

4.0 DOCUMENTATION MANAGEMENT

The Conflict of Interest Register (i010502) and Conflict of Interest Disclosure form (i010501) (which includes management plans as required) will be held within the HR Department. This aligns with the disclosure forms being stored in ConnX as well as forming part of the annual performance appraisal process.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Conflict of Interest Disclosure form (i010501)	Conflict of Interest Register (i010502)

6.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	11 April 2024
Effective Date	23 April 2024	**Document Number**	i010500_v3_240423

(Uncontrolled when printed)

1.2.7 Contract Acceptance and Execution

1.0 INTRODUCTION

To advise the process and outline delegation responsibility for all employees, in particular the Operational Managers, around the handling of all tenders/submissions, contracts, contract variations, MOU's and SLA's. All agreements are legally binding documents and need to be managed in line with Governance principles and practices.

2.0 ACRONYMS

STEPS Group	STEPS
Memorandum of Understanding	MOU
Service Level Agreements	SLA
Managing Director	MD
Chief Executive Officer	CEO
Executive Assistant	EA

3.0 CONTRACTS/MOU/SLA

3.1 ACCEPTING CONTRACTS/MOU/SLA

All contracts, MOUs or SLAs under any STEPS entity must be reviewed, approved, signed and executed by the MD/CEO.

In the instance the MD/CEO is not available to sign the relevant documentation, it is to be forwarded to the approved first line delegate for signing.

Under no circumstance, is an employee of STEPS, including management (except for the approved first line delegate) to sign a contract, MOU, or SLA on behalf of the organisation.

Prior to accepting a contract/MOU/SLA, the office of the MD/CEO are to identify the terms of the contract to be complied with. This will be the responsibility of EA.

3.2 ABANDONMENT OF CONTRACTS

Abandonment of contracts can only occur if both parties mutually abandon the contract. STEPS must perform its obligations in the contract or STEPS may be found to be in breach of contract. If a manager/supervisor is concerned about the ability of STEPS to perform its obligations under a contract, the MD/CEO must be notified immediately.

3.3 TERMINATION OF CONTRACTS

Termination of a contract is a decision made by recommendation to the Board of Directors by the MD/CEO.

3.4 TERMINATION OF MOU's/SLA's

A MOU/SLA usually contains a clause with express conditions on how to terminate the agreement. Only the MD/CEO will be able to exercise this option in accordance with the terms.

3.5 AMENDMENTS TO CONTRACTS/MOU/SLA

Any amendments to existing executed documents under any STEPS entity must be forwarded to the MD's/CEO's EA who will organise review and signing by the MD/CEO.

Once the documentation has been signed and executed, the MD's EA will advise the applicable Manager in writing of the acceptance of the document.

3.6 CONTRACTS REGISTER

The MD's EA will maintain a register for all contracts and communication protocols or guidelines, including renewals and variations, which will record the following details:

- Contract Name
- Start Date
- Expiry Date
- Contact Person
- Reporting
- Review Date.

The EA will forward a copy of approved contracts and amendments to the relevant site contact person.

It is the responsibility of the MD's/CEO's EA to return the approved contract to the applicable government or non-government body for implementation.

4.0 CREATING DOCUMENT FILES

The EA will create an electronic folder and, when applicable, a hard copy file. The electronic folder will be located on 'O' Drive under Contracts.

All contract related documentation is to be scanned and saved under the following relevant subfolders:

- Contracts
- Grants
- Service Agreements

- MOUs and Partnerships.

5.0 COMMUNICATION PROTOCOLS

Government communication protocols are set with the original contract/MOU/SLA stating the MD/CEO as the responsible person. Non-government bodies may have communication guidelines that must be adhered to, however in all instances, the MD/CEO will be the responsible person to manage and execute these documents. Amendments or changes are not permitted by any other employee of STEPS.

All communication regarding performance under any contract such as program assurance, monitoring visits or any other related communications will remain the responsibility of the MD/CEO.

The MD's EA will ensure all relevant employees stated as part of the communication protocols or guidelines will receive written notification of any amendments or changes which may impact STEPS meeting their contractual obligations.

Any changes will be updated via an Organisational System Improvement (OSI) (Corrective Action Register) (i060400) initiated by the MD's EA. The Managing Director will be assigned as the Responsible Person for this OSI. This will ensure all staff will be notified via the STEPS Group OSI Report with the most current Communication Protocol available on the STEPS Quality Manual.

Failure to comply with this direction will be viewed as a serious breach and may result in formal disciplinary action.

DECLARATION

(Please print the Contract Acceptance and Execution (i010900) for employees to read and sign).

Employees must sign this page, retain a copy for their records and return original to the MD's EA.

I, ______________________________________, (employee name) have read, understood, and agree to comply with the Contract Acceptance and Execution (i010900).

Employee Name			
Employee Signature		**Date**	

6.0 RELATED DOCUMENTS

Document Name	Document Name
Organisational System Improvement (OSI) (Corrective Action Register) (i060400)	

7.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	27 July 2023
Effective Date	4 August 2023	**Document Number**	i010900_v3_230804

(Uncontrolled when printed)

1.2.8 Corporate Governance

1.0 INTRODUCTION

The STEPS Group of Companies, STEPS Social Business and STEPS Staffing Solutions (STEPS) Board is responsible for the corporate governance of the Business. Corporate governance is a matter of high importance in STEPS and is undertaken with due regard to all of the business' stakeholders and its role in the community. Corporate governance is not confined to the boardroom, it must be reflected in the culture and business practices throughout the entire organisation (Organisation Chart i010201).

1.1 DEFINITIONS

Compliance	Compliance is adhering to the requirements of laws, industry, government and organisational standards and codes, principles of good governance and accepted community and ethical standards.
Governance	Governance is the activity of governing through decisions that define expectations, grant authority and accountability and verify performance.
Plan	A plan explains the intended actions of the business including the associated coordination details.
Policy	A policy is a statement of the business's position that provides context for procedures.
Procedure	A procedure is a mandatory list of actions to be taken in order to reflect a policy.

1.2 PRINCIPLES OF GOVERNANCE

STEPS governance framework is based on the following best practice recommendations:

a) Lay solid foundations for management and oversight.

b) Structure the Board to add value.

c) Promote ethical and responsible decision-making.

d) Safeguard integrity in financial reporting.

e) Make timely and balanced disclosure.

f) Respect the rights of participants.

g) Recognise and manage risk.

h) Encourage enhanced performance.

i) Remunerate fairly and responsibly.

j) Recognise the legitimate interests of stakeholders.

1.3 GOVERNANCE FRAMEWORK

STEPS governance framework consists of a hierarchy of direction, compliance and audit system, reporting system and a risk management system.

1.4 REGULATORS

Regulators provide obligations to STEPS through the Acts and Regulations. Specific direction is provided by agencies empowered by the Acts and Regulations. Relevant Executive Leadership Managers are responsible for coordinating all communications with regulators and disseminating regulatory requirements throughout the business.

1.5 CUSTOMER

The relationship between the customer and STEPS is established and facilitated through Contracts and Service Agreements.

1.6 BOARD

The Board is responsible for establishing the business's commitment to good governance through example and the implementation of the Constitution. Additionally, it is responsible for the fulfilment of obligations identified by Regulators and the priorities of the customer. The Board communicates its direction for the organisation by the approval of a strategic plan and the annual capital and operational budgets.

The Board has a central role in implementing the organisational values. It will lead by example and while cognisant of risks, it will be pragmatic and decisive in its actions. It will always take pride in working closely with the Executive Leadership Team in seeking excellence across STEPS operations and ensuring this is reflected in STEPS reputation with its stakeholders.

1.7 MANAGING DIRECTOR

The Managing Director, with the Executive Leadership Team, makes decisions regarding governance and provides advice, leadership, and guidance through the approval of plans, strategies, budgets, policies, and processes.

1.8 MANAGEMENT AND STAFF

Management and staff are responsible for carrying out directions in a manner consistent with STEPS obligations, plans, policies and procedures. Management and staff are held personally accountable for their actions.

1.9 RISK AND AUDIT SYSTEMS

Corporate compliance is verified through the risk and audit systems. The risk and audit systems are responsible for:

a) A risk framework, including corporate hazard register.

b) STEPS strategies, plans, policies, procedures, or requirements.

c) Provision of compliance training and advice and support through:

   I. Training needs analysis.

   II. Education programs (coordinated through HR).

III. Advice to managers.

d) Monitoring and reporting on the extent of compliance with the implementation of an internal audit schedule.

All STEPS staff are responsible for reporting possible breaches of the governance framework to a member of Senior Management or an ELT member according to the Fraud and Corruption Prevention and Control Policy (i030400).

1.10 REPORTING SYSTEM

STEPS will establish and maintain a reporting system and will facilitate good governance.

2.0 RELATED DOCUMENTS

Document Name	Document Name
Fraud and Corruption Prevention and Control Policy (i030400)	Induction for Directors (i010401)
Organisation Chart (i010201) *Refer to ConnX*	STEPS Strategic Plan 2016 *(SQM > Reference Documents)*
STEPS Values and Actions (i010402)	

3.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	18 December 2023
Effective Date	2 January 2024	**Document Number**	i010400_v3_240102

(Uncontrolled when printed)

1.2.9 Debt Management & Bad Debts Write Off Policy

BACKGROUND

As part of the management of its financial resources, STEPS Group of Companies (STEPS) needs to ensure that the most effective cash collection procedures are in place and that income generated is reported at the correct levels.

Income to STEPS, is reported through the Profit and Loss Account (P&L) and is calculated to reflect the income generating activity for that time period regardless of whether or not the cash has been received by STEPS (accrual method).

Customers/Clients or Participants do not always pay for the services they have used (e.g., NDIS Managed, Plan Managed, services). If despite best efforts to collect the outstanding income it is deemed to be irrecoverable, it is referred to as an expense not against income.

Treating income as a bad debt should be the final stage of the STEPS debt collection process. To support this, all STEPS Agreements or Contracts provide for the collection of income and is updated and reviewed on a regular basis.

To mitigate against the impact of writing off bad debts, STEPS makes a provision in the accounts (referred to as the bad debts provision).

PURPOSE STATEMENT

The purpose of this document is to outline the policy for the calculation of the bad debt provision and the writing off of bad debts.

APPLICABILITY AND SCOPE

This policy applies to all STEPS staff involved in the raising of income and debt collection activities.

The scope of this policy covers STEPS income across all accounting codes as per the updated Financial Chart of Accounts.

RESPONSIBILITIES

Leadership of this policy lies with the STEPS Executive Leadership Team (ELT).

The Chief Finance Officer (CFO) will be responsible for the management and administration of the policy. The policy will be reviewed on an annual basis to ensure it reflects current accounting practices and is reflective of the financial risks around income collection faced by STEPS.

All STEPS staff involved in the raising of sales invoices are responsible for ensuring that the information contained is correct to reduce the risk of queries and subsequent late payments. They are also required to provide the relevant information and documentation for any debt collection process.

All enquiries relating to this policy should be directed to the CFO in the first instance.

DEFINITIONS

Debtor	A person or organisation that owes money to STEPS.
Bad Debt	An outstanding sum of money owed to STEPS which has not been paid despite repeated efforts to collect the debt (deemed irrecoverable) or it is uneconomic to pursue the debt further.
Bad Debt Provision	This is a provision which is made in STEPS accounts as an operating expense which may not be collectable. It ensures that future period's results will not be adversely impacted if debts need to be written off.
Write-Off	This is a procedure used in accounting when a debtor (or other asset) is determined to be uncollectable and is therefore considered to be a loss.

KEY POLICY ACTIONS

Principles for the Management of Bad Debts

STEPS is keen to maximise its cash collection and in the first instance the debt recovery policy will be followed. Where the income remains outstanding and no payment plan has been agreed the following procedure will be followed:

Debts greater than 90 days and less than $500 may be referred to a debt agency or written off, dependent upon circumstances.

Debts greater than 90 days and over $500 will be referred to STEPS approved debt collection agency. Collection charges are passed on, but not always collected.

Debts greater than 90 days and over $5,000 will be pursued by STEPS approved debt collection agency and may be referred for litigation.

Student Debt: Where a student debt has been written off, the individual's record in the database will have the appropriate debtor flag attached.

Commercial Debt: Where the commercial debt is written off, STEPS may be able to claim GST, if GST was originally included. A copy of the original document and a printout will be made available when completing the BAS return.

CALCULATION OF THE BAD DEBT PROVISION

A bad debt provision will be calculated at the end of each financial month, and posted to the financial statements based on the following calculation:

- Any debts over 90 days – 100% (excluding Government debts)
- Any debts over 60 days – 50%

These threshold amounts will be reviewed regularly to ensure they reflect the natural cycle of debt management processes and are relevant to STEPS business model.

MANAGEMENT REPORTING

To enable the CFO to effectively monitor STEPS debtor levels, a monthly aged debt report will be produced for the Managing Director and the Audit Committee. This will identify movements of debtor balances and contain narrative commentary of key risks, issues, and updates on debt collection activities.

PROCEDURES FOR WRITE-OFF

During the financial year, once it is established that debts are likely to be irrecoverable or uneconomic to pursue further, the debt will be recommended for write-off. This recommendation will be from the Finance Manager, in conjunction with the relevant ELT member, to the CFO. The CFO will report all write-off's and/or escalate to the Managing Director in line with the Delegations Register (i010601).

The Delegations Register (i010601) shows the delegated authority limits for the bad debts write-off. Each proposed bad debt will be presented to the relevant authority for approval.

Write-offs are reported in the monthly Audit Committee and Board Reports detailing all debts written off during the month and any outstanding items requiring approval.

This Policy was ratified by the Board on 30 May 2023.

To access a print friendly version of this Policy please click here.

1.2.10 Delegation of Authority

1.0 INTRODUCTION

This procedure details the processes for requesting and approving changes for both financial and non-financial delegations contained within the Delegations Register (i010601).

2.0 CHANGES TO THE DELEGATIONS REGISTER

Any member of the Executive Management Team (EMT) can request to change financial or non-financial delegations by submitting the proposed changes to the ELT.

The Managing Director (MD) can approve requested changes for financial and non-financial delegations. All requested changes for financial delegations will require ratification by the Board of Directors (The Board).

2.1 COMMUNICATION OF CHANGES

All approved changes will be forwarded to the Quality Assurance & Risk team to update the Delegations Register (i010601) on the STEPS Quality Manual (SQM) and will advise relevant parties via email.

The QST will remove all superseded or out-of-date versions from the SQM and archive.

3.0 RELATED DOCUMENT

Document Name	Document Name
Delegations Register (i010601)	Delegations of Authority RACI Chart (i010602)

4.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	5 November 2021
Effective Date	5 November 2021	**Document Number**	i010600_v2_211105

(Uncontrolled when printed)

1.2.11 Diversity and Inclusion Policy

STEPS Group of Companies (STEPS) is committed to an inclusive workplace which embraces and promotes diversity because we know diversity creates better experiences for individuals, teams, our customers, and the business as a whole.

We believe in treating all people with respect and understanding. We strive to create and foster a supportive and inclusive environment in which all individuals (including customers, participants, students, and workers) feel valued for their own unique capabilities, experiences, and characteristics. This policy includes the Anti-Discrimination & Equal Employment Opportunity Policy (i010102).

At STEPS, diversity means more than just acknowledging and/or tolerating difference. We believe the wide array of perspectives which result from diversity promotes innovation and success by being more creative, flexible, productive, and competitive.

To support diversity and inclusion, STEPS Group of Companies has conscious practices which involve:

- Recognising diversity encompasses differences in ethnicity, gender, language, age, sexual orientation, religious and spiritual beliefs, socio-economic status, physical and intellectual ability, thinking styles, experience, and education.
    - Strategic and business planning which ensure differences and values are recognised, incorporate, and implemented in services.
- Recruiting from different cultural, linguistic, and national backgrounds and providing people with disability and Aboriginal and Torres Strait Islander People's access to employment opportunities to allow our workforce to reflect the communities we serve.
- Engaging with other organisations or bodies with diversity expertise to assist STEPS to meet unique needs.
- Acknowledging all forms of discrimination create and sustain privileges for some while creating and sustaining disadvantages for others.

Diversity is an important resource as it assists STEPS to:

- Improve the connection between workers and our customers, participants, and students, who receive services and supports.
- Improve innovation, creativity and inspire worker engagement and satisfaction.
- Be responsive to customers, participants and students when providing individualised services and supports.

STEPS ensures diversity and inclusion are promoted within the organisation by:

- Focusing on ability and not disability across all sites, services and supports.
- Filling employment opportunities based on merit, Equal Opportunity Employment and Gender Equality.
- Providing information and training to workers on the issues associated with discrimination.
- Consulting with participants, and with the participants consent, their family, carers, significant others, and advocates on the needs of individual participants and planning services accordingly.

This policy was ratified by the Board on 30 May 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here

1.2.12 Fitness for Work Policy

STEPS Group of Companies (STEPS) is a not for profit organisation committed to *making a difference by providing opportunity*.

STEPS recognises its obligations to ensure that workers attending the workplace must be 'fit for work'. A worker's fitness for work may be affected for a variety of reasons including mental health and the adverse effects of fatigue and/or alcohol or other drugs. In application of this policy, STEPS acknowledges its obligations under the Work Health and Safety (WHS) standards, relevant legislation and regulatory requirements.

Drugs and Alcohol

The governing organisational policy on drugs and alcohol in STEPS workplaces is:

- STEPS will not tolerate a workers' consumption of alcohol and/or illegal drugs and/or misuse of prescription drugs while at work.
- Having a blood alcohol content greater than 0.00 while operating STEPS vehicles, plant or equipment at any STEPS workplace is prohibited.
- Being impaired by alcohol and/or illegal and/or misuse of prescription drugs whilst attending any STEPS workplace is prohibited.
- Any employee suspected of having a blood content greater than 0.00 while operating a STEPS vehicle, plant or equipment, or being impaired by alcohol and/or illegal drugs and/or misuse of prescription drugs will be subject to testing.
- The illegal or unauthorised possession, consumption or sale of alcohol and/or drugs of abuse whilst attending any STEPS workplace is prohibited.
- Any worker found to be impaired by a process of drug and alcohol testing or found to be in possession of undeclared alcohol and/or drugs of abuse at the workplace will be managed through a disciplinary process up to and including termination of employment.

Fatigue Management

STEPS recognises that employees suffering from fatigue will have an impact in the workplace, whilst acknowledging fatigue can be caused by both work and non-work related factors. Work factors include extended travel for work, shift work and extended working hours.

Fatigue may cause reduced concentration, impaired coordination, compromised judgement and slower reaction times, ultimately increasing the risk of incidents and injuries. Therefore, STEPS is committed to ensuring fatigue does not become an issue in the workplace through appropriate education, promotion of an effective work/life balance and appropriate rostering of working hours.

Mental Health

STEPS believes that mental health and wellbeing is a key factor in ensuring workers are fit for work. The company strives to establish, promote and maintain the mental health and wellbeing of all workers.

This Fitness for Work Policy is built on the following principles:

- Workers being ultimately accountable for ensuring their own fitness for work;

- Minimising the risk of workers attending the workplace unfit for work through mental health, fatigue, or impairment by drugs or alcohol;
- Providing information and resources to educate workers on the impact of drugs and alcohol, and mental health in the workplace; and
- All supervisors are responsible for identifying and addressing fitness for work and following the supporting procedures to reduce any risk for STEPS workers and customers.

This Policy was ratified by the Board on 28 February 2023.

To access a print friendly version of this Policy please click here

1.2.13 Feedback and Complaints Policy

STEPS Group Companies (STEPS) is a not for profit organisation committed to *making a difference by providing opportunity*.

STEPS aims to consistently provide services that meet customer needs and satisfies applicable statutory, regulatory and contractual requirements.

STEPS understands that quality is ultimately determined by customers, therefore, we encourage feedback, which includes compliments, concerns, suggestions and complaints, all of which provide opportunities for improvement. Anyone can provide feedback or raise a complaint, so it is imperative customers are informed of this process including how the information will be recorded, responded to and resolved.

STEPS will ensure implementation of this policy to:

1. Recognise that feedback and complaints are a primary driver of continuous improvement activities to enable our services to meet the needs of our customers.
2. Provide information through the Feedback Procedure (i040100) and Complaints Procedure (i040500) to all employees to facilitate a fair, prompt and confidential response to complaints, reassuring the customer that improvement is the focus and no retributive action will be taken.
3. Encourage customers and stakeholders to provide feedback and raise complaints. This can be done in any of the following forms:
   - In Person
   - In Writing
   - By Phone
   - Contacting the National Disability Insurance Scheme (NDIS) Quality and Safeguards Commission where NDIS participants can make a complaint about an issue arising out of, or in connection with, the provision of supports or services.
4. Provide support and assistance to customers about how to make a complaint and information about accessing an advocate or support person throughout the resolution process.
5. Provide information to customers on applicable external regulatory bodies as required under regulation or contract.
6. Action all complaints within ten (10) business days from receipt, if a longer timeframe is required, the customer or stakeholder must be kept informed.

This Policy was ratified by the Board on 9 December 2022.

To access a print friendly version of this Policy for display please click here.

1.2.14 Fraud and Corruption Prevention and Control Policy

STEPS Group of Companies (STEPS) is a not for profit organisation committed to *making a difference by providing opportunity*.

STEPS is committed to promoting the highest level of integrity and ethical standards in all business practices. This policy is part of the Fraud and Corruption Framework that includes the Code of Conduct and Ethical Behaviour (e210007); Procurement Procedure [i030100]; Fraud and Corruption Prevention and Control Procedure (i030400); Conflict of Interest Procedure (i010500), Whistleblower Procedure (i090500) and the Accepting Gifts and Benefits Procedure (i010800).

Any type of fraudulent activity and corruption is unacceptable and STEPS will not tolerate it under any circumstance as it will have a detrimental impact on the organisation through loss that can either be financial or reputational, which may also negatively impact workers morale and working environment.

The purpose of this policy and its supporting procedures is to provide a framework for STEPS to prevent, deter, detect and investigate all forms of fraud, and to enable employees to know what to do should they become aware of behaviours that are aimed at falsifying information or have the potential to cause loss.

This policy is built on the following principles:

- Workers are ultimately accountable for their own conduct; the prevention of fraud and corruption is everyone’s responsibility.
- Workers must not engage in fraudulent activity themselves nor support or overlook such activity.
- Workers are responsible for reporting known or suspected fraud, or instances of unethical or illegal behaviour, following the supporting procedures.
- Workers are encouraged to report perceived weaknesses in internal controls (procedures) to their direct supervisor.
- Workers will be provided education on fraud prevention and fraud reporting procedures.
- All supervisors are responsible for both the prevention and detection of any fraudulent activity, therefore, each supervisor must familiarise themselves with areas within their sphere of responsibility where potential fraud may occur.
- Risks assessments will be used to identify where instances of fraud and corruption may occur to ensure control and treatments are recorded.
- Supervisors need to make all contractors aware of their obligations to ensure their work is carried out in accordance with their contractual obligations.
- All details of fraud, or suspected fraud, must be kept confidential to ensure an investigation is not compromised and there is no adverse impact on any innocent party.
- Investigations under this policy will be treated confidentially applying the principles of natural justice, with:
  - A person presumed innocent until proven guilty; and
  - A person suspected of fraud having the right to respond to the allegations.

- The decision to refer any matters to an external agency will be made by the Managing Director.
- Disciplinary action, including dismissal and/or possible prosecution, may be taken against any worker who engages in, encourages or knowingly ignores fraudulent activity, or any worker who makes a false report.

This Policy was ratified by the Board on 28 February 2023.

To access a print friendly version of this Policy please click here.

1.2.15 Health, Safety and Environment Policy

STEPS Group of Companies (STEPS) is a not for profit organisation committed to *making a difference by providing opportunity*.

STEPS is committed to ensuring the health and safety of all its employees, volunteers, clients, contractors and visitors. To achieve this, STEPS has developed Organisational Policies and Procedures that seek to comply with ISO 9001 Quality Management Systems; ISO 45001 Health and Safety Management Systems; ISO 14001 Environment Management Systems; ISO 27001 Information Security Management Systems (ISMS); National Disability Insurance Scheme (NDIS) Practice Standards and Quality Indicators, National Standards for Disability Services (NSDS); National Standards for Mental Health Services (NSMHS) and the Standards for Registered Training Organisations (RTOs).

STEPS recognises the importance of Health, Safety and Environment Management in conducting its daily business. Work Health and Safety is everyone's responsibility. We each have a duty to prevent harm to ourselves and others by identifying hazards and managing risks in our workplace. To achieve this, workers at all levels need to be actively engaged in developing and sustaining a safety culture.

STEPS will ensure implementation of this policy to:

1. Promote health, safety and environment management at all work locations.
2. Plan for and manage hazards to ensure WHS of all workers, clients and relevant members of the public without impact on the environment.
3. Ensure health, safety and environment practices and procedures are implemented and maintained throughout the business; are relevant to the operational activity; comply with statutory requirements; and promote a safe work environment.
4. Ensure appropriate emergency procedures exist in all work locations and that all workers understand the procedures relevant to their location.
5. Provide instruction, training and supervision, dissemination of information and necessary resources to support health, safety and environment.
6. Ensure that there is ongoing consultation and communication with relevant stakeholders.
7. Ensure the establishment of measurable objectives and targets for health, safety and environment to ensure continuous improvement.
8. Provide appropriate protective equipment to comply with statutory requirements and to meet the relevant needs of each area of work activity.
9. Ensure appropriate procedures are maintained for the reporting and review of all health, safety and environment incidents and situations likely to be hazardous to a safe working environment.
10. Ensure appropriate procedures are in place to promote effective workers' compensation claim management and rehabilitation.

All workers have a responsibility to follow all health, safety and environment policies and procedures and to report any hazards.

This Policy was approved by the Chair on behalf of the Board on 11 July 2024.

(Uncontrolled when printed)

To access a print friendly version of this Policy for display please click here.

1.2.16 Operating Reserve Policy

BACKGROUND

The objective of the Operating Reserves Policy for STEPS Group of Companies (STEPS) is to ensure the stability of the mission, programs, employment and ongoing operations of the organisation.

PURPOSE STATEMENT

The Operating Reserve is intended to provide an internal source of funds for situations such as a sudden increase in expenses, one-time unbudgeted expenses, and unanticipated loss in funding or uninsured losses.

The Reserve may also be used for one-time, nonrecurring expenses that will build long-term capacity, such as staff development, research and development, or investment in infrastructure.

The Operating Reserve is not intended to replace a permanent loss of funds or eliminate an ongoing budget gap. It is the intention of STEPS for Operating Reserves to be used and replenished within a reasonably short period of time.

The Operating Reserve Policy will be implemented in concert with the other governance and financial policies of STEPS and is intended to support the goals and strategies already approved by the Board.

APPLICABILITY AND SCOPE

This policy applies to all STEPS senior executive management and the Board of Directors.

The Operating Reserve Fund is a designated fund set aside by action of the Board of Directors.

The Operating Reserve Fund serves a dynamic role and will be reviewed and adjusted in response to internal and external changes.

RESPONSIBILITIES

Leadership of this policy lies with the Chief Financial Officer (CFO) and Managing Director.

The Chief Executive Officer (CEO) will be responsible for the management and administration of the policy. The policy will be reviewed on an annual basis to ensure it reflects current accounting practices.

All enquiries relating to this policy should be directed to the CEO in the first instance.

DEFINITIONS

Operating Reserve Fund	An amount approved to be set aside for strategic purposes.
Average Operating Costs	Includes recurring, predictable expenses such as salaries and benefits including motor vehicles, occupancy, and office and program costs.
Available cash and cash equivalents	Current assets less current liabilities.

KEY POLICY ACTIONS

Identification of appropriate use of the Operating Reserves Fund

The CEO will identify the need for access to reserve funds and confirm that the use is consistent with the purpose of the Reserves as described in this Policy.

The CEO will submit a request to use the Operating Reserves to the Managing Director. The request will include the analysis and determination of the use of funds and plans for replenishment.

The organisation's goal is to replenish the funds within 24 months to restore the Operating Reserve Fund to the targeted minimum amount. If a longer time frame is required, it would be expected a more detailed analysis would be provided.

The Managing Director will approve or modify the request and authorise the transfer and use of funds.

Management Reporting

The CEO is responsible for ensuring that the Operating Reserve Fund is maintained and used only as described in this Policy.

Upon approval of the use of Operating Reserve funds, the CEO will maintain records of the use of funds and plan for replenishment. They will provide regular reports to the Board of Directors on the progress to restore the Fund to the target minimum amount.

Calculation of the Operating Reserve Fund

The target minimum Operating Reserve Fund will be equal to one month of average operating costs.

The Fund will be funded and available in cash or cash equivalents, maintained in a segregated bank account or investment fund.

If the cash or cash equivalents is lower than the target minimum Operating Reserve, then the Reserve will be the cash or cash equivalents balance.

This Policy was ratified by the Board on 30 May 2023.

To access a print friendly version of this Policy please click here.

(Uncontrolled when printed)

1.2.17 Policy Management

1.0 ESTABLISHING THE POLICY FRAMEWORK

STEPS Group of Companies, hereafter referred to as STEPS recognises the importance of documenting and communicating its commitments to standards of behaviour, quality of services and products, management of the environment for its workers, clients, suppliers, contractors, consultants, and others who may be affected by the way STEPS conducts its business.

The commitment and values of the business have been agreed to by the STEPS Board of Directors and expressed in strategic planning and governance procedures. A number of policy statements have been developed to simply express the company's commitment to various objectives arising from the strategic goals of STEPS including its commitment and values.

1.1 DEVELOPING A POLICY

The Directors and Executive Managers will work to develop and document STEPS commitment and values. Policy statements will be derived from commitment and values and will outline STEPS goals and undertakings, be relevant to STEPS overall commitment and objectives and set the framework for a process of continuous improvement.

Policy Statements may include as a minimum, statements regarding:

- Recognition of legislative compliance and obligations
- Recognition of the requirement for continual improvement
- Identification of responsibilities and accountabilities for relevant workers
- Recognition of communication of all relevant information
- Protection of workers and others
- Expectations of all workers
- Recognition of a risk management approach for controlling all hazards
- Incorporation of a commitment to consultation.

1.2 OTHER POLICIES

The Executive Leadership Team (ELT) will work to develop and document additional policy statements as the need is identified. All policy statements must be relevant to STEPS overall commitment and objectives and set the framework for the process of continual improvement. The policy statements will be endorsed by the Managing Director (MD) or nominee and contain a date of issue.

1.3 REVIEW

All policy statements will be reviewed every two years in consultation with workers as required.

1.4 DISPLAY

The Executive Leadership Team (ELT) will determine which policy statements will be displayed at various points at the workplace and within key documents for client information and induction. Points of display will be selected to ensure that the policy statement is highly visible to all persons in and visiting the workplace. The policies to be displayed at sites are Health Safety and Environment Policy (i010101), Feedback and Complaints Policy (i010103), Information Security Policy (6002300) and Safeguarding Policy (i010115). Also, a colour copy of the Complaints Process (i040101) is to be displayed at all STEPS sites that deliver a service to our customers.

1.5 COMMUNICATION

All workers in the workplace will be made aware of the Policy Statement display points and will be made aware of the content and application of all policy statements through appropriate induction and awareness sessions undertaken for the company.

1.6 TRAINING

All such induction and awareness sessions will be undertaken as a part of training and induction.

2.0 RELATED DOCUMENTS

Document Name	Document Name
Anti-Discrimination and Equal Employment Opportunity Policy (i010102)	Change Management Policy (i010113)

Child and Youth Safety and Wellbeing Policy (i010107)	Communication Policy (i010114)
Complaints Process (i040101)	Debt Management & Bad Debts Write Off Policy (i010109)
Diversity and Inclusion Policy (i010112)	Feedback and Complaints Policy (i010103)
Fitness for Work Policy (i010104)	Fraud and Corruption Prevention and Control Policy (i010108)
Health Safety and Environment Policy (i010101)	Information Security Policy (6002300)
Operating Reserve (i010110)	Privacy Policy (i010106)
Quality Policy (i010111)	Safeguarding Policy (i010115)
Workplace Bullying and Harassment Policy (i010105)	

3.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	11 July 2024
Effective Date	17 July 2024	**Document Number**	i010100_v7_240717

(Uncontrolled when printed)

1.2.18 Privacy Policy

Privacy is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination. Privacy includes the right to be able to control who can see or use information about you. Your right to privacy isn’t absolute, sometimes other concerns are given priority, such as the safety of you or others, or the interests of justice.

STEPS Group of Companies (STEPS) complies with obligations under the Privacy Act 1988 (Privacy Act). STEPS is bound by the Australian Privacy Principles (APPs) in the Privacy Act which regulate how organisations collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.

Personal information in the Privacy Act, means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable, STEPS collects, uses, and stores a range of personal information for the purposes of delivering services. Personal information will not be disclosed to third parties without consent, except where permitted or required under the Privacy Act.

The following principles apply within this policy:

- Consent to collect, store and disclose information will be in writing.
- Where possible, STEPS collects personal and sensitive information directly from you. In some situations STEPS may obtain or disclose your personal information to a third-party source. If this occurs, we will take reasonable steps to ensure you are aware of why this information is being shared.
- STEPS only uses personal information for the purposes for which it was given to STEPS or for purposes which are related to STEPS' functions or activities.
- Information collected from clients, business partners, members, donors, members of the public and workers will be limited to that which is relevant and necessary to their involvement with STEPS.
- Any information collected for a particular purpose (the primary purpose) will not be used for another purpose (the secondary purpose) unless:
    - Consent has been received to the use or disclosure of the information; or
    - The individual would reasonably expect STEPS to use or disclose the information for the secondary purpose and the secondary purpose is directly or closely related to the primary purpose.
- On request, clients will be provided with access to an independent support person or advocate of their choice to assist them in all matters relating to the collection, storage, disposal and accessibility of personal information.
- STEPS will manage unsolicited personal information as per the requirements of APP Chapter 4 (Dealing with unsolicited personal information).
- Reasonable access to information held about individuals and to the mechanisms through which any incorrect or inaccurate information can be corrected may be provided upon request.

If an individual does not wish to provide personal information, STEPS may not be able to provide a service.

This Policy was ratified by the Board on 26 April 2023.

To access a print friendly version of this Policy please click here.

1.2.19 Quality Policy

STEPS Group of Companies (STEPS) is committed to maintaining a quality management system in which:

- customer and applicable statutory and contractual requirements are determined, understood, and consistently met,

- risks and opportunities that can affect conformity of services and supports are identified and addressed,
- customer satisfaction is a focus, and
- improvement of services and supports and the effectiveness of the quality management system are continually improved.

To achieve this, STEPS will:

- Communicate its Quality Policy and applicable procedures to all workers and relevant interested parties,
- Periodically review our Quality Policy and procedures to maintain relevance and continual improvement,
- Educate and train our workers to continually improve awareness, skills and knowledge of quality processes including:
  - Where to find information relevant to their role and responsibilities
  - Implications of not conforming with the quality management system requirements
  - Feedback and Complaints
  - Auditing processes
  - Suggestions for improvement
  - Addressing non-conformities
- Setting quality objectives that are reviewed on a regular basis by the Executive Leadership Team (ELT)
- Identifying, reporting, investigating, and resolving all non-conformances and taking action to prevent recurrences.

It is the responsibility of all STEPS workers to implement this Policy to ensure our services and supports satisfy our statutory requirements, standards, contractual obligations and customer, participant, and student expectations.

This Policy was ratified by the Board on 30 May 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here.

1.2.20 Regulatory and Standard Compliance

1.0 MANAGING COMPLIANCE

This procedure describes the processes for ensuring that references to statutory, standards and advisory material relied on by STEPS Group of Companies (STEPS) is current.

2.0 ACCESS TO STATUTES, STANDARDS, CODE OF PRACTICE AND OTHER INFORMATION

All employees have access to Statutes, Standards, Codes of Practice and other information in the Reference Section of the STEPS Quality Manual (SQM).

3.0 REVIEW OF EXISTING STATUTORY AND OTHER REFERENCE DOCUMENTS

Acts, Regulations, Australian Standards and Codes of Practice are recorded in the electronic Legislative Register (i020101). Information contained in the Legislative Register (i020101) will be audited quarterly.

4.0 MAINTAINING RELEVANT STATUTES STANDARDS AND CODES

The following table describes how legislation will be considered and amendments notified within STEPS.

No	Particulars	By whom	By when	Method
1.	Completing a risk assessment of a work process or activity requires a search of relevant legislation, standards, and codes of practice and industry guidelines.	Executive Leadership Team (ELT) or nominated person.	Prior to commencing new work activity of changing a work activity.	General Risk Assessment (i050105)
2.	Conduct search of relevant literature to identify acts, regulations, standards, codes of practice that are relevant to a hazard identified during a WH&S Office Inspection.	Work Health and Safety Officer (WHSO)	On completion of hazard identification	WH&S Office Inspection Checklist (i060201)
3.	Record all relevant acts, regulations, standards, and codes of practice on a Legislative Register (i020101) will be amended as required.	Quality Systems Administration Coordinator	In accordance with the Monitoring / Audit Schedule located in the Quality files Master Audit Schedule (MAS) (i060101).	Legislative Register (i020101)
4.	Update the Legislative Register (i020101) when notified of amendments made to relevant Acts, regulations, standards or codes of practice, through STEPS Quality Systems, internal audit or as advised by STEPS Quality & Compliance Manager or Executive Leadership Team (ELT).	Quality Systems Administration Coordinator	On receipt of notification.	Legislative Register (i020101)

No	Particulars	By whom	By when	Method
5.	Communicate amendments made to relevant Acts, regulations, standards or codes of practice to relevant Executive Manager.	Quality Systems Administration Coordinator	On receipt of notification.	STEPS Quality Systems or email.
6.	Update policies and procedures in response to legislative amendments.	Document owner	As required.	Organisational System Improvement (OSI).
7.	Amendments to legislation are recorded in the Quality & Compliance section of the Executive Manager Shared Services monthly Board Report	Executive Manager Shared Services	Monthly	Board Report

5.0 RELATED DOCUMENTS

Document Name	Document Name
Legislative Register (i020101)	General Risk Assessment (i050105)
Corporate Governance Policy (i010400)	Master Audit Schedule (MAS) (i060101)
WH&S Office Inspection Checklist (i060201)	

6.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	23 September 2021
Effective Date	17 December 2021	**Document Number**	i020100_v2_211217

(Uncontrolled when printed)

1.2.21 Risk Management

STEPS is committed to effectively managing risks to protect its people, assets, reputation, and overall business objectives. This Risk Management Policy outlines our approach to identify, access, evaluate and mitigate risks across the organisation in accordance with the principles and guidelines of *ISO: 31000:2018 – Risk Management*.

STEPS defines risk as “the effect of uncertainty on objectives”. This policy, the Risk Management Framework (i052700) and Risk Management Procedure (i050100) provide information on the processes used to manage risks within STEPS. WHS and individual client risks are managed separately.

This policy is built on the following principles:

- risk management is an integral part of our decision-making processes
- risk management is embedded in all the organisation's practices and processes, including the strategic and business planning and review, and change management processes
- adequate resources will be provided to enable the risk management to be applied and maintained
- encourage proactive management and active participation in risk management, consultation and communication through the engagement of all relevant stakeholders
- risks are evaluated and those risks that need further mitigation are prioritised
- while some risks cannot be eliminated, action is taken to identify risks and remove, minimise or manage them
- the board will be informed of all high and extreme risks.

The Board of Directors/Executive Management will oversee the implementation, effectiveness, and continuous improvement of the risk management framework and processes. The Executive Leadership Team is responsible for ensuring adequate resources are available to maintain the Risk Management Framework.

This Policy was ratified by the Board on 25 July 2023.

To access a print friendly version of this Policy please click here.

1.2.22 Safeguarding Policy

STEPS Group of Companies (STEPS) is committed to upholding human rights as per the United Nations Declaration of Human Rights, 1948 and maintaining a culture that promotes and protects the welfare and human rights of people that interact with or are affected by our work – particularly those who may be at risk of abuse, neglect or exploitation.

All people, regardless of their age, gender, race, religious beliefs, disability, sexual orientation, or family or social background, have equal rights to protection from abuse, neglect and exploitation.

STEPS will promote and protect the interests and safety of children, young adults, vulnerable people and people at risk. We have a zero tolerance of any form of physical and/or sexual abuse.

All employees, volunteers, contractors and third parties of STEPS share responsibility for protecting everyone from abuse, neglect or exploitation.

The purpose of this policy and its supporting procedures [Recognising and Responding to Abuse, Neglect and Exploitation (i051400); Whistleblower (i090500); Risk Management (i050100); Safeguarding Preventing Abuse, Neglect and Exploitation (i052500)] is to provide guidance to employees, volunteers, contractors and third parties as to the action that should be taken when they suspect any abuse within or outside the organisation and provide assurance that all suspected abuse will be reported and fully investigated.

This policy is built on the following principles:

- All employees, volunteers and contractors will uphold people's human rights and work to provide an environment that is supportive of all children, young people, and vulnerable people's emotional and physical safety.
- That all parties will familiarise themselves with STEPS' policy, procedures, Code of Conduct and Ethical Behaviour (e210007) and relevant laws in relation to their responsibilities for identifying possible occasions of physical and/or sexual abuse and for reporting any reasonable belief or

incident that a child, young person or vulnerable person's safety or welfare is at risk to responsible persons in the organisation, or authorities (such as police and/or the child protection services).

- All employees, volunteers and contractors will be provided with Safeguarding training as part of their induction and are required to maintain awareness to understanding, recognise and report an incident, potential incident, or disclosure.
- Risks will be identified and controlled by establishing controls and procedures for preventing and detecting abuse, neglect, or exploitation when it occurs.
- All suspected, perceived, potential or actual incidents must be reported and recorded in the incident management system and will be investigated in a confidential, sensitive, and objective manner.
- A worker, contractor, participant, customer, or student reporting a concern, disclosure or incident will be listened to and will not be victimised.
- If a breach of any policy or procedure is identified at the conclusion of any investigation a worker may be subject to disciplinary action, which may include dismissal and/or reporting to the relevant authority in accordance with mandatory reporting requirements.

This Policy was approved by the Chair on behalf of the Board on 11 July 2024.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here.

1.2.23 Strategic Planning

1.0 INTRODUCTION

STEPS' strategic plan captures decisions made by the board and management that determine how STEPS will meet its goals while responding to changes in the environment and allocating resources to meet those goals.

STEPS undertakes the process of strategic planning with input from different levels of management to assist and enhance the understanding of current performance and the environments in which it operates, and to develop plans for implementing the strategy and a set of measures to indicate how well the implementation is going.

STEPS develops strategic plans on a triennial basis (every three years). These plans are supported by business plans, operational plans and supporting plans. The development of these plans will be shared between board and management and will contain organisational aspirations and the key milestones and objectives needed to deliver the desired results.

SCOPE

STEPS planning will occur in accordance with the financial year and is based on levels of plans to connect long term goals to day-to-day activities. It is a collaborative approach designed to facilitate a deep understanding of current performance and internal and external environments. This procedure outlines the process for developing cohesive plans throughout the business.

PROCESS AND OWNERSHIP

The planning process is owned by the Managing Director who will be responsible for:

- Ensuring the currency of the procedure
- Reviewing the procedure in accordance with quality system requirements
- Facilitating and reporting on the delivery of plans included in this procedure

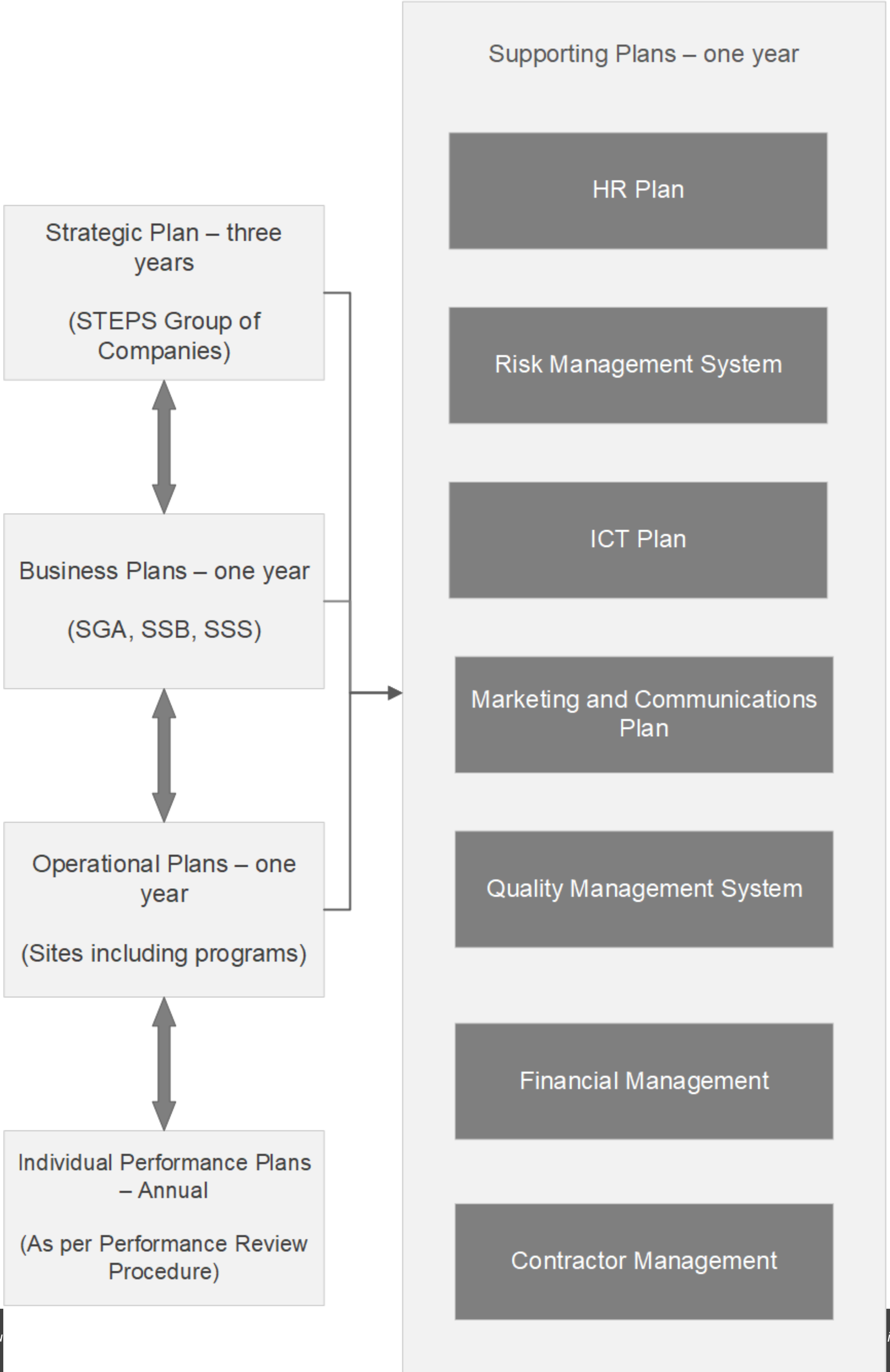
TYPES OF PLANS - COVERAGE AND CONTENT

Strategic Plan	Developed for the STEPS Group of Companies Three yearly cycles with annual reviews Reflect the organisation's purpose (commitment and values) Contain long-term aspirations/future desired state (with a three to five plus year time horizon) Compliant with all legal and regulatory requirements Consideration will be given to risk and outcomes (e.g. quality of care, financial) Key Result Areas to enable the board to monitor performance with any deviation to be explained Finalised before the expiration of the current plan Approved by the board
Business Plans	Developed for each entity within the STEPS Group of Companies, STEPS Group Australia, STEPS Social Business and STEPS Staffing Solutions Annual cycles on the financial year Contain high-level annual and medium-term milestones linked to the strategic plan Measures clear, concise and outcome focused Managers monitor and measure monthly with the board reviewing measures quarterly Presented to the board by June each year for endorsement Following board endorsement, the business plans become operational and reportable in the new financial year
Operational Plans	Developed for each site with consideration to the programs delivered from the site Annual cycles on the financial year, following the endorsement of the business plans Contain short-term objectives that detail the plan for implementation of milestones Key Performance Indicators to measure achievement of objectives

	C level managers review KPIs monthly and share information with the Executive Leadership Team (ELT) Approved by the responsible Chief Operating Officer
Individual Performance Plans	Developed for staff in accordance with the Performance Review Procedure (e220200) Completed annually Contain individual Key Performance Indicators that cascade from the operational plans Includes professional development plans aligned with individual goals and the long-term aspirations of the organisation Approved by the direct line manager / supervisor
Supporting Plans	Developed for each team within corporate services and stated responsibilities Annual cycles on the financial year, following the endorsement of the business plans Contain specific objectives linked to the strategic plan, business plans and operational plans Key Performance Indicators to measure achievement of objectives C level managers review KPIs monthly and share information with the Executive Leadership Team Approved by the responsible C-Level manager

2.0 THE PLANNING FRAMEWORK

The diagram below represents STEPS' planning framework:


Strategic Plan – three years
(STEPS Group of Companies)
Business Plans – one year
(SGA, SSB, SSS)
Operational Plans – one year
(Sites including programs)
Individual Performance Plans – Annual
(As per Performance Review Procedure)
Supporting Plans – one year
HR Plan
Risk Management System
ICT Plan
Marketing and Communications Plan
Quality Management System
Financial Management
Contractor Management

3.0 THE PLANNING CYCLE

Planning requires decisions on direction and how the organisation will meet its goals. Strategy development may be shared between the board and management.

More detailed planning and implementing the strategic objectives is undertaken by management. Management will develop plans to advance the organisation toward its goals and the board will monitor progress toward the desired results.

The commitment to strategic planning is an important basis for accountability and prioritisation of tasks and allocation of resources. Translating strategy to action and the achievement of desired outcomes occurs as information cascades as follows:

1. Strategic plan
2. Business plans
3. Operational plans
4. Supporting plans
5. Annual Individual Performance plans

This top-down approach is informed by the planning process that involves information to flow bottom-up.

The planning calendar is detailed below:

The Planning Calendar:

Month	Strategic Plan Cycle	Business Plan Cycle	Operational / Functional Plan Cycle	Reporting
July	Review strategic planning Processes and templates	Workshops to develop Measurable Outputs for each entity	Plan meetings/workshops for Business planning	Monthly reports for Operational plan and Supporting Plan
August	Plan meetings and workshops	Workshops to develop Measurable Outputs for each entity	Schedule in diaries	Monthly reports for Operational plan and Supporting Plan
September	ELT to approve planning meetings and workshops	Documentation of Plan (approval by ELT)		Monthly reports for Operational plan and Supporting Plan Quarter 3 report on Business Plan
October	Schedule in diaries	**Board endorsement**		Monthly reports for Operational plan and Supporting Plan
November	PESTLE Analysis	Workshops to communicate to managers	Review strategic plan and business plan and collect data to understand current state	Monthly reports for Operational plan and Supporting Plan
December	Reschedule activities if needed.		KPIs drafted in operational and functional plans	Monthly reports for Operational plan and Supporting Plan

				Quarter 4 report on Business Plan
January	SWOT Analysis		Review KPIs against business plans and alignment strategic KRAs	Monthly reports for Operational plan and Supporting Plan
February	Presentation Preparation		'C level' manager to approve plans	Monthly reports for Operational plan and Supporting Plan
March	Strategic Planning Workshop occurs every three years or Strategic Plan Annual Review occurs annually	Plan meetings/workshops for Business planning	Communicate to relevant stakeholders	Monthly reports for Operational plan and Supporting Plan **Quarter 1** report on Business Plan
April	Documentation	Schedule in diaries		Monthly reports for Operational plan and Supporting Plan
May	Plan Approval (by the board)	Review current state and strategic plan		Monthly reports for Operational plan and Supporting Plan
June	Strategic Plan released	Report against progress		Monthly reports for Operational plan and Supporting Plan **Quarter 2** report on Business Plan

Legend:

Stage 1 – Strategic plan (once every three years)	Stage 2 – Business Plans (+ three mnths) completed annually	Stage 3 – Operational and supporting plans (+ six mnths) completed annually	Stage 4 – Implementation and Reporting	Approval of plan	Administration	Communication

STRATEGIC PLANNING (ONCE EVERY THREE YEARS)

The strategic plan will identify strategies to move the organisation from its current state towards a desired future state.

The key elements of strategic planning will include:

- The evaluation of programs that already exist
- The availability and capacity of current resources and the need for additional support
- The impact from the external environment

Tools that can be used for this include SWOT analyses, key issues analysis and to PESTLE analyse to understand different external factors (Political, Economic, Sociological, Technological, Legal and Environmental).

This information will be presented at a strategic planning workshop or retreat. To achieve the optimal results it will be necessary to complete the following steps:

- Before the retreat – management should collate and develop materials incorporating the key items noted above within their area of responsibility discovered during the PESTLE analysis and the SWOT analysis
- Develop a targeted agenda to focus on achieving specific outcomes and resolutions in key decision areas

STRATEGIC PLAN REVIEW (ANNUALLY)

The strategic review will occur annually and will allow for an evaluation on how well each entity is progressing in the goals and objectives that were set for the year.

There are several benefits for a strategic review which include:

- An opportunity for board and management to re-engage with the strategy, bringing the desired future back into focus and renew the sense of purpose
- Clarifying goals and reinforces organisational alignment, promoting teamwork and reminding all managers how they, and their teams contribute to the bigger picture
- Providing an opportunity to build and maintain a strong culture that align actions to values
- Identifying if any changes are needed, opportunities for growth or decisions relating to perceived or actual roadblocks

The board and management will be involved in the review where all will review the big picture in the strategic plan to confirm it is still valid, it will be useful to review any disruption that has occurred in the internal or external environments that may not have been foreseen during the planning phase.

The goal of the strategic plan review is to modify the strategy only where needed, as the strategic plan is long-term in nature and involves big commitments it should remain relatively consistent.

BUSINESS AND SUPPORTING PLANS

STEPS will develop its business and supporting plans using the Planning Template (i040602) annually and will contain the overall outcomes that will be achieved in the following year. Supporting plans will include specific measures and accountabilities to deliver them, the specific actions for business plans will be supported by the key performance indicators for each site.

These plans will be consistent with the key result areas in the strategic plan, stating clear and concise outcome measures that will ensure change is managed effectively. They will provide clarity on what will be delivered and when, and who will be responsible for delivering the change.

OPERATIONAL PLANS

Business plans will be supported by operational plans, which will be completed annually and detail specific KPIs that will demonstrate how the milestones are translating into performance.

Operational plans detail what will occur at a site level and will consider each site’s prior outcomes, current performance and capacity.

4.0 DEVELOPING THE STRATEGIC PLAN

The purpose of the strategic plan is to provide a document that will allow STEPS to move from its current state to a future desired state. The plan will have a three-to-five-year outlook.

STEPS will use the following phases to develop its strategic plan; preparation, planning; monitoring and review.

PHASE 1: PREPARATION

This phase sets the foundation for the planning process. Preparation is important as it provides the opportunity to conduct a systematic and thorough evaluation of the how STEPS operates and the external macro environment. Taking the time to work through this phase will encourage a strategic-thinking mindset and create an awareness of internal and external factors which will provide insight into our current position and will assist in making decisions.

Executive Managers need to build an understanding of the macro-environmental factors that have impact on STEPS and the locations and industries in which we operate. This can be done through a PESTLE analysis which is considered a strategic business planning or market research too that focusses on the external environment and should be completed before the SWOT. PESTLE is an acronym that stands for Political, Economic, Social, Technological, Legal and Environmental factors.

Factor	Consider the following:
Political	Government policy Political stability Funding availability Grant/Deed dates Unemployment regulations
Economic	Local growth or investment Unemployment rates Inflation / interest rates Australian dollar valuations for overseas providers Population growth
Social	Population demographics (e.g. aging population) Changes in lifestyles or trends (e.g. remote/hybrid working) Data on purchasing patterns or availability of funding
Technological	New discoveries and innovations Technology that is becoming obsolete Ensuring NBN coverage to all sites Cybersecurity / protection of Personally Identifiable Information (PII)
Legal	Industry specific regulations Health and safety regulations Employment regulations (Industrial Relations)
Environmental	Changes in supply Waste disposal Energy consumption

	Pandemic / COVID vaccination or restrictions

Complete the PESTLE analysis by:

1. Conduct research into the areas listed above; gather and record information, it may be useful to list current and future factors
2. Brainstorm and individually rate the impact of each of the factors on the business area
3. Identify opportunities and threats for inclusion in the SWOT analysis (eg is there a technological development that will increase efficiencies)

Each business area will complete a SWOT analysis to get a better understanding of the business area's strengths, weaknesses, opportunities and threats. It is recommended that this is done by gathering a group together, including team leaders and stakeholders.

INTERNAL	Strengths (positive parts of your business, things within your control): • What do we do well? • What do we do better than our competition? • What unique assets do we have internally (such as knowledge, background, network, reputation or skills) and externally (such as customers, patents, technology or capital)? • What positive aspects of the business give us a competitive advantage?	Weaknesses (negative factors, things you might need to improve on): • What and where can we improve? • What do our competitors do better? • Where are the gaps in our assets and resources (such as knowledge, cash or equipment)? • Is the thing that sets us apart from our competition obvious? • How can we improve business processes?
EXTERNAL	Opportunities (positive factors that may give a competitive advantage and contribute to success): • What trends can we use to our advantage to increase use of our product or service? • Are there any changes or events that might positively impact us (such as consumer behaviour, regulation, policies or new technology)? • Has anything changed in the market that creates opportunity for us? • Do the public like us?	Threats (factors beyond your control that may put our business at risk): • What factors beyond our control could place us at risk? • What potential competitors may enter the market? • Are our resource and material supplies unstable or insecure? • Are there any changes or events that might negatively impact us (such as consumer behaviour, regulation, policies or new technology)?

To develop strategy from the SWOT consider asking:

- How can we use our strengths to take advantage of our opportunities?
- How can we use our strengths to minimise our threats?
- What do we need to do to overcome and minimise our identified weaknesses?
- How are / will our customers be impacted by our strengths or weaknesses, are they likely to spend their money with STEPS (creating revenue)?

At the end of this stage, each business area will have proposals/options for what the future could look like and some key decisions needed to decide which direction to take. To assist the strategic planning workshop to reach decisions, it will be helpful if each area of the business considers:

- Who are the stakeholders on which we are dependent (such as government departments, drivers of funding, such as NDIS
- Who are our "target customer/s" (be specific, not people with disability looking for work but people who can work between 8 and 30 hours per week)
- what the organisation needs from each stakeholder group (including what we want from employees) and
- what each stakeholder wants from STEPS.

Please note the idea is not to present certainty and remove risk, it is to make a choice and increase the chance of success by managing risks (not eliminating the risk).

PHASE 2: STRATEGIC PLANNING WORKSHOP

At this workshop, managers will be asked to present information on the current position of the business area/s and internal and external issues that have been identified.

The main activity of this phase will be the consolidation of the provided information, summary of the decisions made and identifying the 5 (+/-2) key result areas KRAs that will form the agreed overall requirements that support the implementation of the strategic plan to achieve the desired outcomes.

When the plan is approved by the board it will then be used to develop the business, operational and supporting plans.

PHASE 3: MONITORING AND REVIEW

Performance against the strategic plan will be monitored through the progress of the business, operational and supporting plans.

An annual review will be held to summarise progress toward the KRAs and to check that no significant external or internal shifts have occurred that make the strategic plan invalid.

5.0 DEVELOPING BUSINESS PLANS

The purpose of the business plans for each entity is to identify and document the outputs expected by each entity in the following fiscal year, they also act as a way of measuring progress toward the strategic KRAs.

PHASE 1: STRATEGIC DIRECTIONS INTO MEASURABLE OUTPUTS

The strategic plan contains the KRAs that will move STEPS toward its desired future and this will provide the focus and direction for business planning.

To set measurable outputs, the leadership team for each entity will consider:

- Current activities

- Customer and staff feedback (bottom-up communication)
- Current capacity and capabilities
- Financial constraints

It is important to note that the outputs may be the achievement of a milestone toward a longer-term goal (i.e. not the end-state).

PHASE 2: DOCUMENTATION AND AUTHORISATION

The business plan for each entity will be documented on the Planning Template (i040602) and will be presented to the ELT for approval and the board for endorsement.

PHASE 3: MONITORING AND REPORTING

Each quarter information will be gathered from an area of responsibility and consolidated by each C-level manager to be able to report on the progress toward the business plan.

This information will be included in the board reports in:

1. January (for Oct-Dec);
2. April (for Jan-Mar);
3. July (Apr-Jun); and
4. October (Jul-Sep).

6.0 DEVELOPING OPERATIONAL AND SUPPORTING PLANS

The purpose of the operational and supporting plans is to specify what each site and corporate service area will deliver in the coming fiscal year. Supporting plans will be completed by a specific corporate service area and will be focussed on the organisation's needs and the needs of the department.

These plans will:

- Align with the strategic and business plan/s
- Expressly state what the site/department will deliver (KPIs) to support the desired future and achieve the business plan milestones (tip is action and detail-oriented)
- Assist in the identification, assessment and treatment of risks

Operational and supporting plans work best when each site or team is included in the development and assigns tasks with due dates.

DOCUMENTATION AND AUTHORISATION

All operational and supporting plans will be developed using the Planning Template (i040602).

Once finalised by the team the relevant 'C' level manager will approve the plan.

MONITORING AND REVIEW

Each manager will present monthly reports on progress toward the KPI.

Larger tasks may benefit from a project plan.

7.0 RELATED DOCUMENTS

Document Name	Document Name
Performance Review Procedure (e220200)	Planning Template (i040602)
STEPS Strategic Plan 2016 *(SQM > Reference Documents)*	Strategic Plan Annual Review for 2022-2023 (i040601)

8.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	18 December 2023
Effective Date	2 January 2024	**Document Number**	i040600_v3_240102

(Uncontrolled when printed)

1.2.24 Vaccination Policy

STEPS Group of Companies (STEPS) is a not-for-profit organisation committed to *making a difference by providing opportunity*.

STEPS is committed to its work, health and safety duty of care to ensure, as far as reasonably practicable, the health and safety of its Workers and others in the workplace. It is acknowledged that work undertaken in certain environments or under the condition of program funding guidelines may require workers to be vaccinated against preventable diseases and these requirements are outlined on relevant role descriptions.

STEPS recognises that preventable diseases may be highly transmissible and dangerous and that vaccination against these diseases is a safe and effective measure to minimise exposure to and spread of preventable disease. For this reason, STEPS recommends all Workers consider vaccination against preventable diseases such as COVID-19 and Influenza. This policy includes the Disability Services in Accommodation during COVID-19 Procedure (i052300), Infection Prevention Procedure (i052000) and Managing Suspected or Confirmed Cases of Infectious Diseases (i051900).

STEPS recognises that some Workers are required to have close contact with people who are particularly vulnerable to the health impacts of preventable diseases. Where there is frequent interaction between Workers and other people such as customers, other Workers or the public in the normal course of employment, STEPS recommends Workers consider vaccination against preventable diseases such as:

- Measles
- Mumps
- Rubella
- Varicella (Chicken Pox)
- Pertussis (Whooping Cough)
- Hepatitis B

- COVID-19.

This policy applies to all Workers (permanent, specific period or casual), labour hire personnel and volunteers who may be performing work at any of STEPS' workplaces in Australia (Workers) excluding offsite events.

STEPS encourages Workers to consider following current advice from the Australian Technical Advisory Group on Immunisation (ATAGI) regarding dose and booster frequency where relevant.

Managers must:

- Ensure that all Workers are aware of and understand this policy.

Workers must:

- Consider seeking their own independent medical advice as to the potential health effects involved in receiving protections against vaccine preventable diseases.
- Continue to comply with any other safety protocols in place to minimise exposure to vaccine preventable diseases.

STEPS will be continuously monitoring and assessing the operation of this policy in line with the latest information from Government and health authorities. STEPS may amend, withdraw, or replace this policy from time to time at its sole discretion.

This Policy was ratified by the Board on 28 May 2024.

1.2.25 Whistleblower

1.0 INTRODUCTION

This procedure provides a guide on how STEPS will support people to confidentially raise concerns about service delivery in the interests of service safety and quality and for the prevention and detection of all forms of fraud from the Fraud and Corruption Prevention and Control Procedure (i030400). It will support whistleblowers, who in good faith and without malice, disclose information or raise concerns about alleged improper or illegal activity. For examples of what may be considered improper or 'reportable conduct' please refer to the Fraud and Corruption Prevention and Control Procedure (i030400).

The information in this procedure applies to all workers including permanent and casual, contract workers, temporary agency workers, and volunteers.

STEPS and our employees are committed to providing services in a safe and honest way. We expect everyone to comply with all legal requirements. We will support and respect anyone who acts as a whistleblower to draw attention to suspected inappropriate, corrupt or illegal conduct or behaviour.

1.1 DEFINITIONS

Whistleblower	A person who raises concern regarding illegal and/or improper conduct that affects others. The person is not usually involved in the issue but is wanting to alert others to suspected misconduct. The alert may be raised outside of usual reporting lines or processes.
Reportable Matter	Reportable matters refer to information about misconduct, fraud, corruption and other improper business activity or systemic issues which pose a risk of harm to staff, consumers or the organisation. For a matter to qualify for whistleblower

	protection under the Corporations Act, the information should be about the organisation, or an employee or officer, engaging in conduct that: • breaches the Corporations Act • breaches other laws enforced by ASIC or APRA • breaches an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months, or • represents a danger to the public or the financial system. Disclosable matters can include conduct that may not involve breach of a particular law. Disclosures can also include information of activity which poses a significant risk to public safety or which risks the stability of, or confidence in STEPS, or in public entities, even if it does not involve a breach of a particular law.

2.0 WHISTLEBLOWER RIGHTS

To encourage whistleblowers to come forward with their concerns and protect them when they do, the Corporations Act 2001 (Corporations Act) provides certain protections for someone making a disclosure if they meet certain qualifying conditions. Qualifying conditions and protections are outlined below.

2.1 QUALIFYING AND DISQUALIFYING CONDITIONS

A person making a disclosure will be eligible for protection as a whistleblower if:

a) they have shared information on a matter which is considered reportable conduct outlined in the Definitions in section 1.1 above; and

b) they have reasonable grounds to suspect the matter being reported. The whistleblower will not be expected to prove their allegation however should present supporting information which demonstrate reasonable grounds of suspicion.

Disclosures relating to personal work-related grievances do not qualify for whistleblower protection under the Corporations Act. Personal work related grievances are defined as matters which do not relate to reportable conduct and which do not pose a risk of harm to the individual disclosing. Examples of matters which would not qualify for whistleblower under the Corporation Act include grievance about interpersonal conflict, decisions made about work roles which do not breach employment laws. Work-related grievances can still qualify for whistleblower protections if the work-related grievance also includes a breach to employment laws or a reportable conduct.

Work-related grievance can be reported to following the Employee Grievance Procedure (e210100).

3.0 PROVIDING INFORMATION

3.1 HOW TO MAKE A DISCLOSURE

Reporting Internally

In order to qualify for whistleblower protection under the Corporations Act, reports must be made to an eligible recipient. At STEPS an eligible recipient includes members of the Executive Leadership Team (ELT), the Managing Director (MD), or a member of the Board.

Information can be provided in any format. Claims made in conversation will be documented by the person receiving the claim. The record of conversation must be signed by the whistle-bower to verify it is a true account.

This signed copy will be stored securely accessible only by the person who received the disclosure. A copy will be made with edits which protect the whistleblower identity.

Where an employee has acted as a whistleblower, the person receiving the disclosure will discuss the matter with a member of the ELT or the MD taking due care to de-identify the information, and uphold the whistleblowers rights to confidentiality. The whistleblowers identity must not be disclosed to anyone.

To protect the person’s identity, the following steps should be taken:

- all personal information or reference to the discloser witnessing an event will be redacted;
- the discloser will be referred to in a gender-neutral context; and
- the discloser will be contacted to help identify certain aspects of their disclosure that could inadvertently identify them.

External Reporting Options

A disclosure can be made to an external party. These external reports can be made to auditors, ASIC, APRA or another Commonwealth body such as:

Australian Skills and Qualifications Authority (ASQA) Info Line on 1300 701 801, Monday to Friday, between 9.00 am and 7.00 pm Eastern Standard Time (EST).

Department of Social Services the best place to lodge your disclosure at: *https://www.dss.gov.au/contact/feedback-compliments-complaints-and-enquiries/contacts-page*

In Queensland, if the disclosure relates to the health or safety of a person with a disability contact the Queensland Ombudsman, the relevant Public Sector Agency you believe has the authority to investigate the matter or any Member of Parliament.

3.2 PROTECTIONS AND SUPPORTS FOR WHISTLEBLOWERS

Confidentiality

A person making a disclosure can choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalised. To maintain their total anonymity, the whistleblower can use an anonymous telephone line or anonymous email address when making a report to the eligible person. Alternatively a confidential disclosure can be made to an eligible recipient (as above).

A person making a disclosure who wishes to remain anonymous is encouraged to maintain ongoing two-way communication with the person they disclosed to so the person can ask follow-up questions or provide feedback. This whistleblower can refuse to answer questions that they feel could reveal their identity at any time, including during follow-up conversations.

Whether submitting an anonymous submission or not, the identity of a whistleblowers will not be shared with anyone without the whistleblowers consent. Information which is likely to reveal the identity of the whistleblower will not be shared without the whistleblowers consent.

To protect the person’s identity, the following steps should be taken:

- all personal information or reference to the discloser witnessing an event will be redacted;
- the discloser will be referred to in a gender-neutral context; and
- the discloser will be contacted to help identify certain aspects of their disclosure that could inadvertently identify them.

Staff who feel there has been a breach to confidentiality can lodge a complaint by following the Employee Grievance Procedure (e210100).

Protection from retribution and disadvantage

A whistleblower will also be protected from disadvantage, harm and retribution which could result from the act of reporting the matter. This will include upholding the STEPS Code of Conduct and Ethical

Behaviour (e210007) and could also include ensuring the whistleblower is not subject to dismissal, position changes or reputation damages related to having made a disclosure.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Code of Conduct and Ethical Behaviour (e210007)	Complaints Procedure (i040500)
Employee Assistance Program (e230100)	Employee Grievance Procedure (e210100)
Feedback Procedure (i040100)	Fraud and Corruption Prevention and Control Procedure (i030400)
Privacy Policy (i010106)	Work Health & Safety Incident Investigations (i090300)

5.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	5 October 2021
Effective Date	12 October 2021	**Document Number**	i090500_v4_211012

(Uncontrolled when printed)

1.2.26 WHS Responsibilities and Accountabilites

1.0 ESTABLISHING RESPONSIBILITIES AND ACCOUNTABILITIES FOR WHS MANAGEMENT

STEPS Group of Companies (STEPS) has identified the importance of establishing legal, ethical and moral responsibilities and accountabilities of workers within the scope of their authority for WHS. STEPS recognises the crucial role that the Managing Director, the Board and the Executive Leadership Team (ELT) have in driving WHS and the importance of leadership commitment to health and safety principles that assist the organisation in achieving its goals in the wider marketplace in which it operates.

2.0 ORGANISATION STRUCTURE AND PLANNING FOR WHS

The Managing Director, the Board and the ELT will develop and maintain a current Organisation Chart (i010201) that depicts the various levels of WHS responsibility and accountability within the organisation. The Quality Objectives Plan (i010301) will be developed and maintained that gives effect to the efficient and best practice management of the WHS based on the organisation chart.

3.0 DEVELOPMENT AND REVIEW OF RESPONSIBILITIES AND ACCOUNTABILITIES

The Managing Director, the Board and the ELT will work to develop and document responsibilities and accountabilities for positions depicted in the Organisation Chart (i010201) and shown in Work Health Safety (WHS) Position Responsibilities and Accountabilities Statements (i010202). Each Role Description (RD) statement will outline the responsibility and accountability for the role and must be relevant to the company's overall commitment and objectives and state the legal, ethical and moral accountabilities for the position.

Responsibility and accountability statements are established in each RD, approved by the Managing Director and contain a date of issue. The document is discussed with the relevant employee.

The Work Health Safety (WHS) Position Responsibilities and Accountabilities Statements (i010202) will be discussed during the annual performance review process with all employees.

4.0 REVIEW

WHS status will be reviewed using the Reviewing Work Health Safety (WHS) Status (i060200).

Performance appraisals will be undertaken of all employees and managers as required in the Performance Review Procedure (e220200).

5.0 RELATED DOCUMENTS

Document Name	Document Name
Performance Development Review (e220203)	Performance Review Procedure (e220200)
Organisation Chart (i010201)	Work Health Safety (WHS) Position Responsibilities and Accountabilities Statements (i010202)
Reviewing Work Health Safety (WHS) Status (i060200)	

6.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	1 June 2023
Effective Date	5 June 2023	**Document Number**	i010200_v2_230605

(Uncontrolled when printed)

1.2.27 Workplace Bullying and Harassment Policy

STEPS is committed to promoting courtesy, respect and trust, and a workplace environment that is free from bullying and harassment.

Bullying occurs where a person (or group of people) repeatedly act unreasonably toward another person (or group of people). Acting unreasonably includes behaviours that may be considered victimising, humiliating, intimidating or threatening (e.g. acting aggressively, teasing, practical jokes, excluding someone). It is important to note, that reasonable management action carried out in a reasonable way is not bullying (this may be making decisions about poor performance, taking disciplinary action or directing or controlling how work is carried out).

Harassment can include behaviour such as telling insulting jokes (e.g. about particular racial groups), comments, emails or text messages that are sexually suggesting or explicit, displaying offensive pictures or screen savers, making derogatory comments or taunts about a person's disability, or asking intrusive questions about someone's personal life (e.g. someone's sex life).

Bullying and harassment is unacceptable and STEPS will not tolerate it under any circumstance, or in any form including cyberbullying. Cyberbullying is simply, bullying or harrassment that is conducted with the use of technology, like mobile phones or the internet.

Any form of bullying can have a detrimental effect on our organisation and individuals. Bullying or harassment may cause the loss of customers or workers, reduced productivity, reputational damage among customers or potential customers, loss of profits, low morale, increased complaints or grievances and create legal risks and costs for our business.

STEPS expects all workers, customers, participants and students to act in accordance with the following legislation: Sex Discrimination Act 1984, Racial Discrimination Act 1975, Disability Discrimination Act 1992, Age Discrimination Act 2004, Australian Human Rights Commission Act 1986, Work Health and Safety Act 2011 and Fair Work Act 2009.

The purpose of this policy and its supporting procedures Feedback Procedure (i040100); Complaints Procedure (i040500); Employee Grievance Procedure (e210100); Preventing and Responding to Bullying and Harassment Procedure (i050700) is to provide the framework for compliance with the legislation and to enable workers, customers, participants and students to know what to do should they become aware of workplace bullying or harassment.

This policy is built on the following principles:

- Workers, participants, customers and students are ultimately accountable for their own conduct.
- Workers, participants, customers and students are protected by this policy whether they feel bullied or harassed by another person or group of people they should report the matter, following the supporting procedures (listed above).
- Workers, participants, customers and students will be provided with information and/or training in relation to workplace bullying and harassment and the procedures for making a complaint.
- All workers have a responsibility to identify and address conduct that may constitute bullying or harassment, including conduct that occurs between participants, customers or students.
- Supporting procedures provide a seamless link between reporting, investigating and determining solutions for bullying and harassment matters.
- All reports of bullying and harassment will be taken seriously and responded to promptly, impartially and confidentially.
- Investigation of any breaches of this policy will be treated sensitively and conducted in a robust and objective manner.

- A worker, participant, customer or student making a complaint and/or a witness to bullying or harassment will not be victimised.
- A worker who is found to have breached this policy or a worker who makes a vexatious or malicious complaint may be managed through a disciplinary process.

This Policy was ratified by the Board on 28 February 2023.

To access a print friendly version of this Policy please click here.

1.3 Corporate Management

Enter topic text here.

1.3.1 Change Management

1.0 INTRODUCTION

As a "for purpose" organisation STEPS is always looking for ways to *make a difference by providing opportunity* and this often comes in the form of improving existing services and infrastructure, delivering new services, or expanding services into new geographic regions.

1.1 PURPOSE

The ultimate goal of change management is to drive organisational results and outcomes by engaging employees and inspiring them to adopt a new way to achieve results.

To maximise the benefits from change whilst minimising disruptions and negative or unintended consequences STEPS aims to approach change in a coherent and planned manner. Complex change involving support functions of the organisation will be strengthened using structured project management processes.

The types of change events that STEPS is likely to experience includes but is not limited to:

- Changes in scale – where new tenders or grants are awarded, mergers occur, or new sites are opened.
- Changes in structure or staffing – from time-to-time it will be necessary to adjust staffing levels, organisational structure or key supervisory or management roles, all of which may impact team dynamics and team performance.
- Changes in technology – where information and communications technology require updating or equipment changes to provide the required level of reliability and security of the ICT infrastructure. Please refer to the ICT Change Management Procedure (6002400) for more detail.
- Changes in service offerings – when new services are added or improvements in current operating processes are introduced existing employees may need training. Additional employees may need to be recruited, new premises opened, or new equipment introduced.
- Regulatory and Compliance changes – shifts in laws, regulations or contracts can have significant impact on how work is undertaken.

2.0 CHANGE PROCESS

Changes may impact people, processes and technology and it is important that STEPS manages change well through a defined change management process that involves the following stages:

2.1 IDENTIFYING THE NEED FOR CHANGE

STEPS encourages all workers to consider how:

- Services can be improved when they reflect on their experience in delivering services (including things like service models, infrastructure, technology, responsibilities, communication, knowledge)
- the experiences of our customers, participants, or students in receipt of services and the feedback they provide may be improved.
- Workers may also receive requests for services that we do not currently provide which may indicate a need in the community that is not being met.

Managers must consider how:

- New or changing regulatory or contractual obligations may require changes in current processes, reporting, service delivery etc
- Improvement in performance for a program, service or site can be achieved

Corporate Services can support change requests from others across the organisation in addition to using their own knowledge and experience to continually improve productivity, performance, and efficiencies for the organisation as a whole.

2.2 INITIATING THE CHANGE REQUEST

All workers can initiate change utilising a variety of mechanisms including:

- various ticketing systems, for example OSI, ICT Helpdesk
- raising suggestions with their manager,
- raising an online Innovation Idea form
- completing a Project Proposal (i010713) that sits within the Project Management Procedure (i010700) and associated Framework of processes, forms and templates.

2.3 A REVIEW OF THE CHANGE REQUEST

Regardless of the channel through which the change idea has been initiated, the idea will be reviewed by the Change Committee which will apply a set of criteria to determine its size, complexity and potential impact for STEPS. These criteria are fully laid out in the supporting Project Management Framework Summary (i010702) and Project Management Procedure (i010700), and the Project Sizing Guide (i010715).

There are four ‘status’ of ideas that are progressed through this review stage, which will determine the level of support to be provided to the idea:

Emergency: Where the need is determined by outside factors and the timescale to address it is either immediate or determined by an outside body. Examples might include a breach of data security, a business continuity action following a natural disaster, a sudden change in regulatory requirements under which STEPS operates.

Business as Usual (BAU): Operational activities that drive and sustain routine, everyday work within STEPS.

Small Project: A minor internal project that requires change to a process, configuration of an existing system or related reporting. These could be tactical or operational in nature, possibly connected to a continuous improvement initiative.

Project: A significant undertaking – outside the everyday operations and resources of STEPS, likely to be strategic in nature – building new capabilities, such as services, facilities or markets. Building or improving business-critical systems and infrastructure would also be examples here.

2.4 CHANGE ASSESSMENT, EVALUATION AND CLASSIFICATION

The Change Committee will be responsible for combining their knowledge and experience to assess or evaluate the change to understand the alignment with the strategic values, direction, benefits, consequences, effect on overall performance, impact on information security and risks, as well as the potential investment in funds and resources required.

The Change Committee will classify the Change Requests as either:

- An emergency, BAU, Small Project or Project.
- For all classifications other than BAU, the Change Committee will document the discussion in the format of the Project Proposal (i010713) and may include its collective input, where required, to the point that it can be presented to the Executive Leadership Team (ELT) with its recommendation.

2.5 CHANGE RESOURCES

The Change Committee will also consider what resources will be required to implement the change and identify if internal resources have the capacity and capability to make the change or if external resources will need to be brought in to undertake all, or parts of the change process.

2.6 APPROVAL OF THE CHANGE REQUEST

The Change Committee will provide the Executive Leadership Team (ELT) with the change request information, possibly including a Project Proposal (i010713), including its assessment and evaluation and recommendation regarding resources.

The ELT will be responsible for approval of the change.

2.7 PLANNING

Each approved change, regardless of whether it is BAU or a project, will need to have the following as a minimum:

- a vision of the change that is aligned to the strategic objectives,
- a documented statement of the benefits the change will deliver, often achieved through knowing the current position and the desired future position (e.g., a gap analysis)
- identified resources required to achieve the change objectives.
- A communication plan. It is well accepted that change is often unsettling for employees, for this reason it is important that employees are engaged and motivated to support the change. This is often achieved through explanation of why the change is happening and the benefits of the change. Good communication (including feedback) is a significant part of any change plan or project.

2.8 DELIVERING THE CHANGE

The Project Management Framework Summary (i010702), overseen by the Project Management Office (PMO), has published processes, guidance, forms and templates for the ongoing management of the initiative through this ideation/initiation phase through to completion.

For changes delivered using business as usual (BAU) activities such as team meetings or performance reviews the relevant line manager/supervisor will need to provide monthly updates to the PMO, on the progress towards delivering the desired future state as stated in the plan.

The delivery of projects other than BAU initiatives, will be executed by an appointed Project Manager or Leader, adopting proven approaches and progress will be monitored using project performance reporting in accordance with planned reporting dates. This reporting will include progress and completion of scheduled project activities, budget management, risks and issues, and the associated change and communications plan. These progress reports will be collated by the PMO and distilled into consolidated reports for the ELT and the STEPS Board of Directors.

1.0 CHANGE COMMITTEE

3.1 FUNCTIONS OF THE CHANGE COMMITTEE

The Change Committee will provide governance of the change management processes in STEPS. This will be achieved by:

- recording and assessing/evaluating the change requests
- classifying the change requests
- providing ELT with information and recommendations to support decisions regarding approval
- providing assistance and support when requested by those responsible for implementing the change
- Collating reports on progress and success to promote accountability and transparency, through the office of the PMO

The Change Committee will involve members from different teams including PMO, ICT, Finance, HR, Operations, and other members as appropriate.

3.2 CHANGE COMMITTEE MEETINGS

The Change Committee will meet bi-weekly in accordance with the Terms of Reference, to discuss new initiatives being proposed and receive updates and feedback from the ELT on submissions presented.

Minutes of meetings will be maintained.

3.3 CHANGE REPORTING

The PMO will be responsible for reporting on the following:

- The number of change requests received each month.
- The number of change requests referred to ELT.
- The number of change requests approved and rejected.
- Progress of project plans and/or changes.
- Completion of projects and/or changes.

Outcomes of reviews for each project and/or change.

4.0 PROCESS FOR CHANGE REQUESTS

4.1 NARRATIVE FOR CHANGE REQUESTS

Please refer to the Project Management Framework Summary (i010705) and Project Management Procedure (i010700) for the detailed process.

4.2 PROCESS ROLES AND RESPONSIBILITIES

CHANGE INITIATOR (ANY STAFF MEMBER)

- Responsible for identifying the need for a change and providing the required information to allow the change request to be assessed.
- May work with the Change Committee to define the exact requirements of the change.

CHANGE COMMITTEE

- Support the governance of change within STEPS.
- Assess, evaluate, and classify major change requests.
- Work as a team and invite input from other internal stakeholders to understand the change request and its requirements.
- Use Project Management Framework Summary (i010705) to develop Business Case (i010707) / Project Proposal (i010713) and define scope and resources, where needed.
- Consult with ICT Team to understand impact and risks to information assets that may be affected by the change.
- Provide information to ELT for approval.
- Communicate with change initiator.
- Identify and propose an Executive Sponsor.
- The PMO will support the implementation of the change once approved.

EXECUTIVE LEADERSHIP TEAM (ELT)

- Approve changes presented that align with the strategic values, direction, meet business needs and conform to change management processes.
- Confirming the priority of approved changes/projects.
- Verify where possible that resources are committed to executing approved changes/project to agreed schedules.
- Resolve conflicts in the change/project schedule.
- Taking corrective action against any person/group who attempts to circumvent the change management process.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Business Case (i010707)	ICT Change Management Procedure (6002400)
Innovation Idea	Project Management Framework Summary (i010702)
Project Management Procedure (i010700)	Project Proposal (i010713)
Project Sizing Guide (i010715)	

6.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	6 April 2023
Effective Date	14 April 2023	**Document Number**	i011200_v2_230414

(Uncontrolled when printed)

1.3.2 Effective Meetings

1.0 ELEMENTS OF EFFECTIVE MEETINGS

Effective meetings can be described as meetings that:

- Achieve the meeting’s objective
- Take the minimum amount of time required, and
- Leaves participants feeling that their time at the meeting was worthwhile.

1.1 THE MEETING OBJECTIVE

An effective meeting serves a useful purpose. This means that in it, you achieve a desired outcome. For a meeting to meet this outcome, or objective, you have to be clear about what it is.

Consider what you want the outcome to be before you call a meeting. These could include:

- Do you want a decision?
- Do you want to generate ideas?
- Are you getting status reports?
- Are you communicating something?
- Are you making plans?

1.2 TERMS OF REFERENCE

Terms of Reference (ToR) (i040402) can be used to set out the working arrangements for a meeting and can list vital information, such as its purpose, chair and membership, meeting schedule, level of administrative support, and dispute resolution processes.

A Terms of Reference (ToR) (i040402) should be a short document to assist in the:

- Integration different sources of knowledge and information needed for a specific purpose (e.g. project, program delivery)
- Allow for evaluation of achievements
- Ensure any regulatory requirements are met, and
- Satisfy industry standards.

1.3 USING TIME WISELY

Everything that happens in the meeting should further the objective, if it doesn't, it's superfluous and should not be included.

To ensure you cover what needs to be covered and you stick to relevant activities, you need to create an agenda. The agenda is what you will refer to in order to keep the meeting running on target and on time.

1.4 MEETING ETTIQUETTE

It may be helpful for your meeting to follow a set of “ground rules,” or etiquette, that govern the way you behave.

These ground rules will vary according to your management style, and the preferences of your team.

Etiquette covers behaviors such as timekeeping; the use of laptops and cell phones; eating and drinking during the meeting; whether you can interrupt while someone is speaking, or only ask questions at the end; where you sit, and so on.

Some meetings may be more formal than others, depending on the agenda and who is attending. But agreeing to these basic standards – and sticking to them – can help you and your team to conduct meetings in a more professional manner, and to achieve your objectives with the minimum disruption, keep to time and have people leaving the meeting feeling that it was worthwhile.

2.0 PREPARE AN AGENDA

To prepare an agenda, consider the following factors:

- Priorities – what absolutely must be covered?
- Results – what do you need to accomplish at the meeting?
- Participants – who needs to attend the meeting for it to be successful?
- Sequence – in what order will you cover the topics?
- Timing – how much time will spend on each topic?
- Date and time – when will the meeting take place?
- Team Name?
- Location – where will the meeting take place?
- Who will take the minutes or will this be assigned at the time of the meeting
- For site meetings – WHS & OSI must be included

- Ensure there is an assigned Minute Taker

Now you know what needs to be covered and for how long, you can then look at the information that should be prepared beforehand.

What do the participants need to know in order to make the most of the meeting time? And, what role are they expected to perform in the meeting, so that they can do the right preparation?

If the meeting objective is to solve a problem ask the participants to come prepared with a viable solution. If you are discussing an ongoing project, have each participant summarize his or her progress to date and circulate the reports amongst members.

Assigning a particular topic of discussion to various people is another great way to increase involvement and interest. On the agenda, indicate who will lead the discussion or presentation of each item.

Use your agenda as your time guide. If the chair notices that time is running out for a particular item, consider hurrying the discussion, pushing to a decision, deferring discussion until another time, or assigning it for discussion by a subcommittee.

Use the Meeting Agenda / Minutes Template (i040401) and record your agenda on the first page using agenda numbers and bullet points to identify key topics and subtopics. If a particular participant will be responsible for presenting a particular items include their name in brackets after the item and be sure to advise them prior to the meeting.

2.1 CIRCULATE THE AGENDA

Once you have an agenda prepared, circulate it to the participants, if time allows get their feedback and input.

Running a meeting is not a dictatorial role, for people to be engaged it helps if participants are engaged from the start are participative from the start.

If you have time to seek feedback, it provides the opportunity to consider if something important should be added, or maybe something can be removed for discussion outside the meeting.

3.0 MANAGING THE MEETING

During the meeting, to ensure maximum satisfaction for everyone, there are several things you should keep in mind:

- If certain people are dominating the conversation the chairperson to, make a point of asking others for their ideas.
- At the end of each agenda item, quickly summarize what was said, and ask people to confirm that that's a fair summary. Then make notes regarding follow-up.
- Note items that require further discussion.
- Meetings should be kept to meeting time allocated.
- Watch body language and make adjustments as necessary. Maybe you need a break, or you need to stop someone from speaking too much.
- List all tasks that are generated at the meeting on the Meeting Agenda / Minutes Template (i040401). Make a note of who is assigned to do what, and by when.
- At the close of the meeting, quickly summarize next steps and inform everyone that you will be sending out a meeting summary minutes of the meeting.

4.0 MINUTES

After the meeting the Minute Taker will send the minutes to attendees.

Minutes provide a summary of the meeting and should be forwarded to all participants. Make sure someone is assigned to take notes during the meeting if you think you will be too busy to do so yourself.

In the table that follows the Agenda on the Meeting Agenda / Minutes Template (i040401) you can type directly into the table in the number that corresponds with the agenda item, or if you prefer you can add sufficient space in the table using the return key and hand write notes.

After the meeting the Minute Taker will send the minutes to attendees.

4.1 ACTIONS

Minutes are a record of what was accomplished and who is responsible for what as the team moves forward. This is a very crucial part of effective meetings as it is a written record of what was discussed, along with a list of actions that named individuals have agreed to perform and the due date.

As you are recording a summary of the discussion document agreed actions or decisions so they can be carried forward to the next agenda to ensure reporting on progress occurs.

5.0 IMPROVING EFFECTIVENESS OF THE MEETING

After the meeting, take some time to debrief, and determine what went well and what could have been done better. Evaluate the meeting's effectiveness based on how well you met the objective. This will help you continue to improve your process of running effective meetings.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Meeting Agenda / Minutes Template (i040401)	Terms of Reference (ToR) (i040402)

7.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	03 September 2019
Effective Date	4 September 2019	**Document Number**	i040400_v1_190904

(Uncontrolled when printed)

1.3.3 Project Management

1.0 PROJECT MANAGEMENT

1.1 INTRODUCTION

Project management is an approach to initiating, planning, managing and delivering approved change in an organisation. The STEPS Project Management Framework Summary (PMF) (i010702) is a suite of processes and forms that have been designed to capture all necessary information at each stage of the project lifecycle, and to allow the project to be successfully delivered.

The PMF is designed to be easy to navigate and easy to support by the PMO, understanding that projects can vary widely in size, complexity and duration….. so a one-size-fits-all approach is not practical.

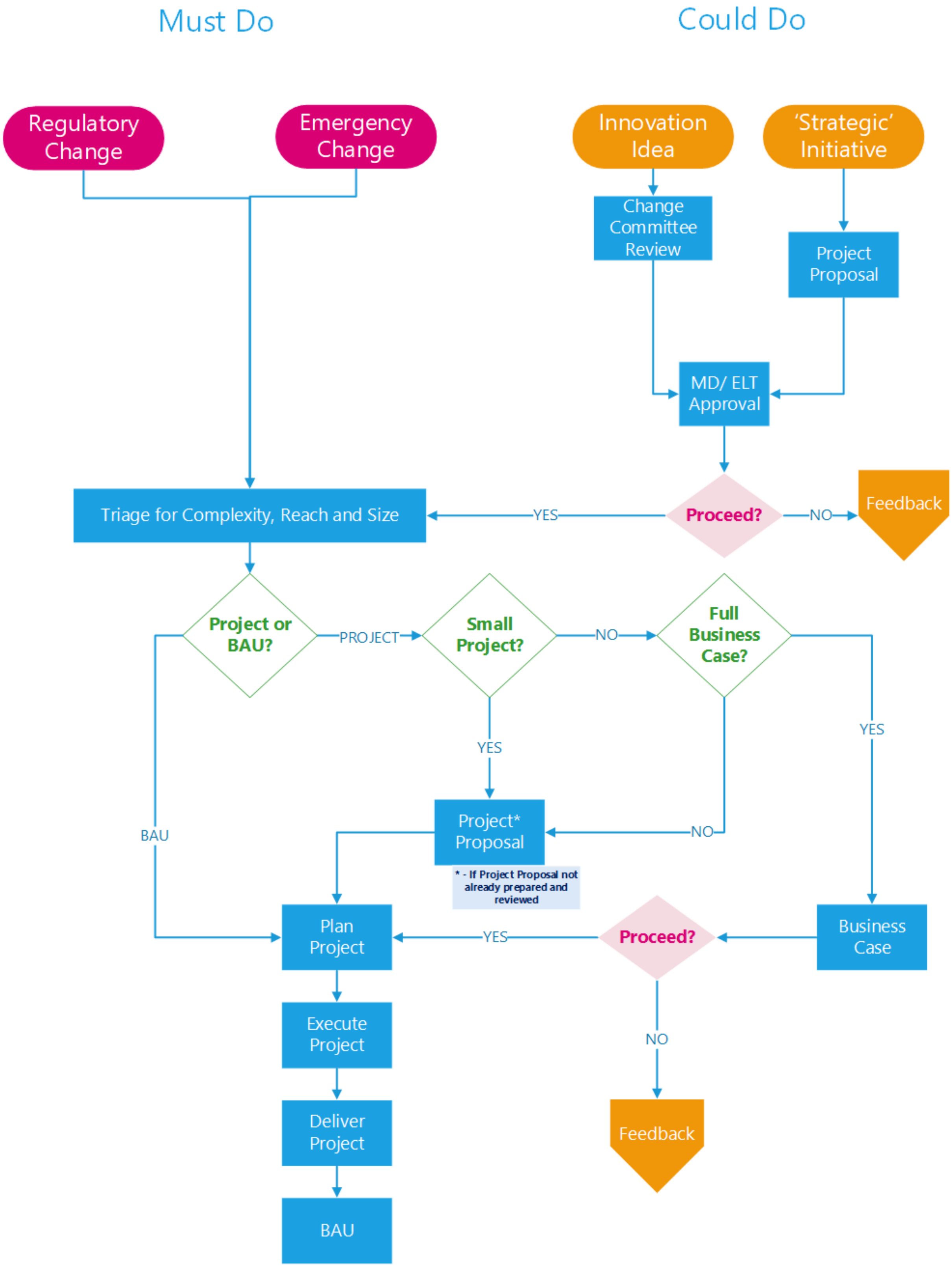
And some changes need to be introduced urgently, under “Emergency” conditions, whereas most would be introduced with longer consideration and decision-making cycles.

Change can be introduced into an organisation from a range of sources:

- Regulatory or Legal Compliance requirements
- Strategic objectives flagged by the STEPS Board or Executive
- At an individual or departmental level as an Improvement Initiative

The STEPS PMF has multiple entry-points for initiating a project. The figure below identifies that there is a “Must Do” stream… where there is an emergency that needs to be addressed, or there is a legal or regulatory change that is mandated. The “Could Do” stream shows that initiatives may grow from anywhere within the organisation – either as a continuous improvement initiative or through strategic decision making. This “Could Do” stream requires a few more steps of analysis and approval before a project is kicked-off.

Figure 1: The general flow of the PMF to illustrate this.



1.2 DEFINITIONS

Project	A unique set of activities (that sit outside of everyday operational activities) required to be completed to achieve a certain objective and/or benefit within an agreed scope, timeframe, budget, and resource allocation.
STEPS Executive	Managing Director and Executive Leadership Team (ELT) – either jointly or severally
Business As Usual (BAU)	Operational activities that drive and sustain routine, everyday work within STEPS, usually undertaken within the resources and authority of a single Business Unit or Stream.

1.3 PROJECT LIFECYCLES

There are four "Flavours" of project that we can identify at STEPS and are defined in the Project Sizing Guide (i010715). These four "Flavours" are:

BAU: Where the execution of the change is regarded as within the budget, resources and authority of a single Business Unit or Stream and the impact of the change on other parts of STEPS is minimal. Reference should be made to the Project Sizing Guide (i010715) to determine if the initiative should be classed as a "Small Project" to ensure it receives the level of support required to make it a success.

EMERGENCY: Where the driver of the change is a set of conditions imposed on STEPS at short notice, or is a response to an issue or Force-Majeure condition. Examples might include a severe weather event, or a cyber-attack, or a pandemic, or the sudden withdrawal of services from a key supplier. Such a situation will require a much shorter timeframe for decision-making and mobilising resources to meet the situation.

SMALL PROJECT: One step beyond a BAU initiative, in that the change may be relatively small scale and minor in impact but will require some changes to processes and systems, and they will require input and effort from other areas of the STEPS business, including the ICT Department. Regular updates to most systems are required, and these updates are managed by the ICT Department under their ICT Change Management Procedure (6002400).

PROJECT: Where an initiative requires specific leadership and allocation of resources to bring it to life. The scale, impact and duration of the project will determine the information that the STEPS Executive will require to provide 'comfort' to their decision making.

The scale, impact and duration of the initiative will determine how much information should be provided to the STEPS Executive to assist their decision making. The PMO will guide the initiator through a Project Proposal (i010713), and then may ask to build on that information with a full Business Case (i010707) if the STEPS Executive feels that is necessary.

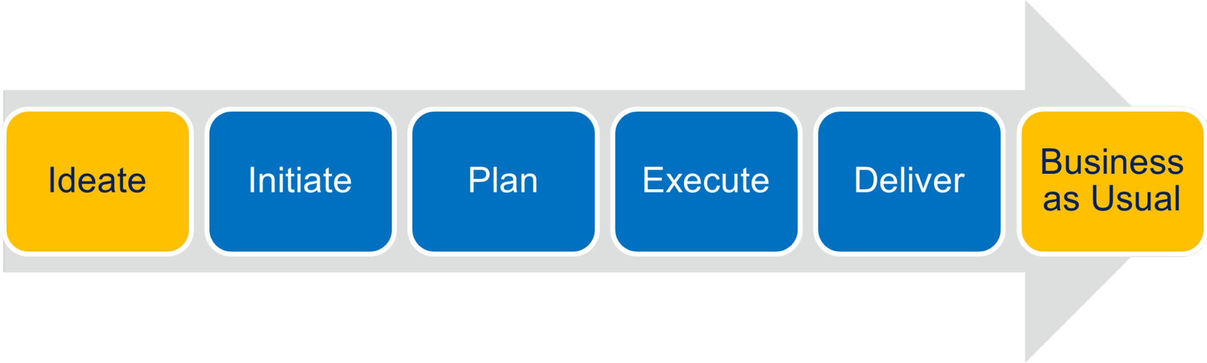
The Project Management Framework Summary (i010702) provides the structure and tools to allow STEPS to move through the Project Lifecycle, as shown in Figure 2 below.

Four project governance forms Innovation Idea, Project Proposal (i010713), Business Case (i010707) and Project Closure & Handover (i010712)) are supported by templates for the Project Plan (i010709), Project Progress Report (i010714), General Risk Assessment (i050105), Project Budget Tracker (i010718) and Project Change Request (i010711).

The document set is designed to be scalable to provide 'just enough' controls and governance, without imposing over-burdensome structure or overhead in managing the project.

This document set will allow all projects, of any size and duration, to pass through the different stages of the PMF in a controlled and referenceable way; To provide a guide for project initiators and sponsors to keep their project on-track, aiming for a successful conclusion.

Figure 2: STEPS' four stage project management lifecycle between the idea being registered and it successfully becoming part of Business as Usual.



2.1 PROJECT DOCUMENTATION

Each document puts the author in the driving seat as to how much information is captured, how much time is spent capturing, validating, and refining the information and how many other people are involved in the process.

As the project unfolds, edits, additions and/or deletions may be required in different parts of the document to maintain its currency and transparency.

Lifecycle Stage	Document Sections	Operational Project Overview
Ideate	Innovation Idea	**may take as little as 30 minutes to complete.** **captures basic information about the idea, the potential change to make, and how that might be achieved.** **submitted to, and reviewed by the Change Committee.**
	Project Proposal (i010713)	**when giving feedback on an Innovation Idea, the Change Committee may suggest to an initiator that their idea would be better presented to the STEPS Executive for feedback and approval with more detail, as captured in a Project Proposal (i010713). Change Committee members could work with the initiator to develop the Project Proposal (i010713) with the required details.**
Initiate	Project Proposal (i010713)	initiator may decide that more information can be submitted about the initiative, and that it should be presented to STEPS Executive directly for review and approval, due to the potential scale and impact of their idea. the PMO can work with the initiator to provide the templates and support to develop their Project Proposal (i010713).

	Business Case (i010707)	more detailed than the Project Proposal (i010713), but building on the information contained in the Proposal; with a greater level of analysis, research and supporting data to justify the size of the investment being requested, records additional information regarding scope (in-scope and out-of-scope), risk, stakeholders, communication, resources, quality and contractual considerations, significant focus on the benefits and Return on Investment to be delivered by the initiative, approval will confirm the investment to be made, the resources and timescales expected and release the project's progression to the 'plan' stage
Plan	Project Plan (i010709)	if the Business Case (i010707) {or Project Proposal (i010713)} outlines the "what" of the initiative, the Project Plan (i010709) details "how" that will be achieved enables a complete breakdown of the project to identify all the agreed activities required to deliver the project successfully creates a timeline of the scheduled delivery, including key milestones throughout the project indicates the allocated resources to be involved, and the extent of their involvement documents how progress, quality, budget, risk, change, communications and decision-making will be managed
Execute	Project Progress Report (i010714)	takes the elements of the Project Plan (i010709) and puts them into practice monitoring of project performance – deliverables, budget and timescales – regularly, on an agreed schedule outlines risks to be managed and decisions-required provides a confidence-level of the ingoing project objectives will be met, or alternatively, a forecasting of variance against those objectives
	Project Change Request (i010711)	identifies proposed change (and owner), records change justification, assesses the impact from the change, confirms the change request has been approved
Deliver	Testing and Commissioning Plan (i010716)	details how the new capabilities, created by the project, will be put in to live operation – whether it as a new service, a new office, or a new computer system. identify how the business owner will test and 'operationalise' the new capability, to ensure that it meets the project objectives and is 'fit for purpose'. document the change management plan for how the new capability will be introduced into the Business-as-Usual environment – testing, training, communications, transition tasks for instance
Complete	Project Closure & Handover (i010712)	confirming the objectives have been met, handing over the deliverables, reviewing timeframe and budget details, reporting the benefits achieved and yet to be achieved, recording lessons learned

3.0 TRACKING ACTIVITIES IN THE PROJECT PLAN

Tracking of project activities is essential and can be achieved in a number of ways. For instance, a simple project task list can be developed in Microsoft Excel, this can be converted into a Gantt Chart for a graphical view. Alternatively, Microsoft Project, or the web-based Project Planner. It is recommended that each project establishes a Microsoft Team, via the PMO, to share and collaborate on project documentation (see below). In each Team it is possible to create the project plan, allocating tasks to the individuals on the project and monitoring progress in a collaborative way within the Team.A Project Schedule (i010717) template is provided for this purpose.

4.0 RECORDING PROJECT DOCUMENTATION

When a project is approved by the Executive, the PMO will request that a Team will be set-up for the project, with the name format - Project-xxxxxxxxxx. The Project Manager, or Project Leader will be nominated as an owner of that Team.

Team members will be added and documents can be stored and shared on the Team 'Files'. A suggested structure for the Team would be to have a "Discussions and Decisions" and a "Plan and Activities" channel in each Team. In addition to the standard "General" channel. This will allow for some segregation of activities and material on the Team. The Project Manager / Leader will be able to structure the Team in a way that makes sense for that project… adding channels and/or tabs as required.

At the end of the project, once the new capabilities have been delivered into BAU, the project Team will be closed and all documentation will be securely archived by the ICT team, via a Helpdesk ticket.

5.0 PROJECT MANAGEMENT FRAMEWORK SUMMARY

The Project Management Framework Summary (i010702) provides a representation of the component parts of the STEPS Project Management Framework including stage objectives, approvals, and key activities.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Business Case (i010707)	Change Management Procedure (i011200)
General Risk Assessment (i050105)	ICT Change Management Procedure (6002400)
Project Budget Tracker (i010718)	Project Change Request (i010711)
Project Closure & Handover (i010712)	Project Management Framework Summary (i010702)
Project Plan (i010709)	Project Progress Report (i010714)

Project Proposal (i010713)	Project Roles & Responsibilities (i010719)
Project Schedule (i010717)	Project Sizing Guide (i010715)
Testing and Commissioning Plan (i010716)	

7.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	6 April 2023
Effective Date	13 April 2023	**Document Number**	i010700_v4_230413

(Uncontrolled when printed)

1.4 Human Resource Management

Contact us

Please email your queries through to HR@stepsgroup.com.au or contact us via 07 5458 3096.

Your HR team

Contact	Availability	Position	Direct Phone
HR Team	Mon - Fri	For all general HR enquiries	(07) 5458 3096 (preferred number)
Mellesa Lee-Smith	Mon - Fri	Executive Manager - Human Resources	(07) 5458 3008 / 0457 896 887
Katelyn Brinkman	Mon - Fri	HR Advisor	(07) 5458 3005
Toni Kriewaldt	Mon - Fri	HR Operations Manager	(07) 5458 3007
Rebecca Devery	Mon - Fri	HR Support Officer	(07) 5458 3014

Hayley Warburton	Mon - Fri	Talent Acquisition and Experience Partner	(07) 5458 3020
Adrian Hayes	Tues, Wed, Thurs	WHS Officer	(07) 5458 3041 / 0447 188 838

For all other related Procedures & Documents, refer to the Human Resource Management Chapter link.

1.4.1 Accepting Gifts and Benefits

1.0 INTRODUCTION

Gifts and benefits may be offered out of goodwill for a job well done. However, gifts and benefits can also be offered as a subtle form of influence to create a favourable impression or to gain preferential treatment. STEPS Group of Companies (STEPS) is committed to upholding the rights of people who access our services.

This procedure has been developed to ensure transparency and that the principles of integrity and accountability in regards to gifts are practiced by all employees, volunteers, board members and other members of the organisation.

1.1 DEFINITIONS

Gift	Free or heavily discounted items or intangible benefits exceeding common courtesy that are offered to employees in association with their work. They range in value from nominal to significant and may be given for different reasons including token of gratitude at the completion of an event.
Benefit	Benefits are preferential treatment, privileged access, favours, or other advantage offered.
Nominal Gift or Benefit	Any item, travel, hospitality, entertainment, or other token of appreciation with a value of less than $50.00.
Reportable Gift or Benefit	An item, travel, hospitality, entertainment, or other token of appreciation with a value of more than $50.00; or
Monetary/Financial Gift	Gift directly to an employee of money or financial benefit. All STEPS Employees must not accept monetary/financial gifts under any circumstances related their employment.
Conflict of Interest	A conflict of interest or the perception of a conflict of interest can arise from gaining personal advantage by receiving gifts or benefits.

1.2 EXCLUSIONS

The following items are excluded from the procedure:

Donations	Money, services, or items donated to STEPS Group Australia.

2.0 ROLES AND RESPONSIBILITIES

2.1 STEPS COMMUNITY SUPPORT EMPLOYEES

STEPS Community Support employees, volunteers or other representatives of the organisation are not at any time to accept or offer any form of gifts including but not limited to cash, valuables, white goods, furnishings, clothing or any other items to clients, their carers, family, or friends.

It is also not acceptable to enter into an agreement to purchase or sell an item to a client, their carers, family, or friends.

If a client is insistent that an employee is to accept a gift, the employee should respectfully decline and suggest and support the client to donate the item to a relevant charity.

2.2 DIRECTORS, MANAGERS, EMPLOYEES, CONTRACTORS AND CONSULTANTS

Employees must not:

- Solicit for private purposes any benefit in connection with their official function and duties;
- Accept any benefit for any official function or duties, performed or not performed, which could create a conflict of interest (refer to Conflict Interest Procedure i010500) or be seen to create such conflict;
- Accept any gift of money or benefit by way of loans and the like for any functions or duties, performed or not performed, which are part of the normal duties of an employee of STEPS.

To remove any ambiguity, this means that a single unsolicited token of appreciation (more than one gift would become a 'series of gifts') below the value of $50 may be received within these guidelines, by an employee from a person who is a beneficiary of the services that STEPS provides.

3.0 CIRCUMSTANCES IN WHICH A GIFT OR BENEFIT MAY BE ACCEPTED

Employees may accept a token gift of gratitude from a group of individuals at the completion of an event where appropriate, never during, but must be declared in writing to the employees Supervisor who will notify the Executive Administration Manager (EAM) and for recording on the Reportable Gifts Register (i010801 - refer to EAM).

In the case of entertainment, moderate acts of hospitality, minor presentations of no significance and nominal value items generally used for promotional purposes, which conform to industry norms:

- employees have exercised judgement in determining whether receipt of a gift could be seen by others as an inducement which could place that employee under an obligation to the donor or associated parties,
- the employee advises their supervisor, or higher authority, of the circumstances and the benefit.

For reportable gifts, authority must be obtained in writing from the employee's Supervisor or higher authority and the gift recorded in the Reportable Gifts Register (i010801 - refer to EAM) by following the process below.

These provisions should not be construed as prohibiting the pursuit of financial assistance or benefit to STEPS where such pursuit is authorised by law.

4.0 PROCESS FOR REPORTING GIFTS

The employee will within 24 hours of the gift being received, notify their supervisor in writing.

The Supervisor will inform the EAM, or delegate who will maintain a Reportable Gifts Register (i010801 - refer to EAM) made to or received from an employee.

The Register of Reportable Gifts will list:

- Description and estimated value of the gift
- Basis for the valuation of the gift
- Date the gift was received
- Authority for retaining the gift or reason for returning the gift
- Identity of the person or party receiving the gift
- Identity of the person or party making the gift
- Any relevant file references
- In the case of reportable gifts received the present location of the gift or the application of the proceeds.

5.0 BREACHES

Any transaction resulting in the exchange of the above-mentioned items may result in disciplinary action.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Reportable Gifts Register (i010801) *Refer to EAM*	Conflict of Interest (i010500)
Fraud and Corruption Prevention and Control Policy (i010108)	

7.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	1 February 2024
Effective Date	9 February 2024	**Document Number**	i010800_v3_240209

(Uncontrolled when printed)

1.4.2 Awards and Enterprise Agreement

This section contains the various industrial instruments (e.g. Awards, Enterprise Agreement) that apply to STEPS Group Australia's employees and numerous Procedures that relate to the terms and conditions of employment.

Awards

Clerks - Private Sector Award (e210012)
Education Services (Post-Secondary) Award (e210002)
Gardening and Landscaping Services Award (e210018)
Labour Market Assistance Industry Award (e210025)
Miscellaneous Award (e210003)
Nursery Award (e210004)
Social, Community, Home Care and Disability Services Industry Award (SCHADS) (e210016)

Enterprise Agreements

STEPS Group Australia Northern Territory Adult Migrant English Program Enterprise Agreement 2021-2022 (e210015)

Fair Work Information Statements

Fair Work Information Statement (e2100019)
Translated Fair Work Information Statement (e210026)
Casual Employment Information Statement (e210020)
Translated Casual Employment Information Statement (e210027)
Fixed Period Information Statement (e210028)

National Employment Standards

National Employment Standards (e210017)

1.4.3 Criminal History Checks

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to meeting its legislative and statutory requirements by ensuring that relevant criminal history checks are held by all employees on commencement and reviewed as required.

DEFINITIONS

Word	Definition
Employee	Means any staff engaged by STEPS, a contractor or subcontractor, trainee, a work experience student, a volunteer.
Customers	Means all students, clients, participants, customers and all other people engaging with STEPS for the provision of goods or services.
Criminal History Check	Means National Police Check and any state or territory check associated with NDIS service provision or working with children.
Specified supports or services	Means services delivered to NDIS participants that are listed in the National Disability Insurance Scheme (Practice Standards – Worker Check) Rules 2018.
Regulated activity	Is defined per paragraph 5 of the Registration to Work with Vulnerable People Act 2013 (TAS).

Responsible Officer	Means the Executive Manager – Human Resources.
Risk Assessed Role	Means under the National Disability Insurance Scheme (Practice Standards – Worker Check) Rules 2018: a) a key personnel role of a person or an entity; b) a role for which the normal duties include the direct delivery of specified supports or specified services to a person with disability; or c) a role for which the normal duties are likely to require more than incidental contact with a person with disability.

2.0 POLICY STATEMENT

STEPS has a responsibility to:

- Ensure the safety and security of employees and customers who rely on and/or receive services provided by STEPS.
- Maintain the security of employee and customer information held by STEPS.
- Treat current and prospective employees fairly in relation to any consideration of their suitability for employment with STEPS.
- Ensure that assessments and decisions made about whether to appoint a person to perform the duties of a particular job in STEPS are consistent, based on the principles of merit and allow for natural justice.

3.0 RESPONSIBILITIES

3.1 EMPLOYEES AND PROSPECTIVE EMPLOYEES

- Complete all required criminal history checks as required.
- Provide relevant proof of identity to accompany the request for a criminal history check.

3.2 MANAGERS AND TEAM LEADERS

- Ensure all documentation in relation to criminal history checks is managed in accordance with this procedure and other relevant STEPS policy and procedure.
- Ensure employees are accountable for actioning renewal notices in accordance with this procedure.

3.3 HUMAN RESOURCES

- Ensure all documentation in relation to criminal history checks is managed in accordance with this procedure and other relevant STEPS policies and procedures.
- Ensure the requirement for conducting a criminal history check is included in all role descriptions.

- Determine whether further criminal history checks are required for employees who have changed roles.
- Ensure information provided by employees and prospective employees is in line with the Fit2Work requirements.
- Review criminal history check results and notify the Responsible Officer of any disclosable outcomes.
- Update the human resource information system as required.
- Facilitate the initial processes for National Police Checks and where relevant setting renewal reminders.
- Review the effectiveness of this procedure, following the policy effectiveness and adherences measures.

3.4 RESPONSIBLE OFFICER

With the relevant Executive Leadership Team (ELT) member:

- Determine, following the criminal history assessment process, whether an individual should or should not be appointed to a role, move to a new role, continue in a current role, or is suitable for continued employment with STEPS because of their criminal history check.
- Consider human rights when making decisions about criminal history checks and recommendations made through the assessment process.

4.0 REQUIREMENTS FOR CRIMINAL HISTORY CHECKS

All employees are to have, at a minimum, one form of criminal history check. Annexure A identifies in what circumstances employees may require different criminal history checks.

An offer of employment is conditional upon the return of acceptable criminal history check(s). Prospective employees must not commence work in the proposed role prior to satisfying this requirement.

STEPS complies with state and Commonwealth legislative and regulatory requirements relating to employment checks in specific areas of employment as follows:

- Working with Children (Risk Management and Check) Act 2000 (QLD).
- Care and Protection of Children Act 2007 (NT).
- The Care and Protection of Children (Check) Regulations 2010 (NT).
- Registration to Work with Vulnerable People Act 2013 (TAS).
- National Disability Insurance Scheme (Worker Check) Act 2020 (Cth).

Reference to employment check requirements relevant to the role must be made when the vacancy is advertised.

Current employees may be required to undertake additional criminal history check when moving into a different role (e.g. secondment, higher duties, promotion, transfer, etc.) that has additional legislative requirements. Current employees must not commence the proposed different role prior to satisfying this requirement.

4.1 CRIMINAL HISTORY CHECK RENEWALS

Annexure B outlines the procedures for applying for renewing a criminal history check. As provided for in paragraphs 3.1 and 3.2, employees are responsible for ensuring that all compliances remain current while managers are accountable for their employees' compliances remaining current.

Employees who do not maintain the currency of their compliance requirements (as outlined in their Role Description) will not be able to attend work until compliance requirements are met.

4.2 CONFIDENTIALITY

Criminal history check information and documentation about a person's criminal history must only be used in assessing the suitability of a person to perform the duties of a role.

Any employees participating in employment check processes, including those providing administrative support, must be made aware of their obligations for privacy and confidentiality and compliance with this policy.

Criminal history information must be managed in accordance with privacy requirements in the Information Privacy Act 2009.

4.3 NON-DISCLOSURE

A person must not be asked to disclose their personal criminal history information to a selection panel or other employee at any stage during a selection process or through the course of their employment.

5.0 CRIMINAL HISTORY ASSESSMENT

A disclosable outcome does not automatically exclude an individual from working at STEPS. An applicant's criminal history that provides a disclosable outcome will be assessed based on a risk management approach and the relevance of an applicant's criminal history information. In determining the suitability of an applicant or employee to perform the relevant duties of a role, the Responsible Officer and the relevant ELT member must consider a number of factors in their decision-making process, including:

- Any legislative requirements which provide automatic exclusion from employment in specific areas for certain offences
- The relevance of the offence to the duties of the job to which it is recommended the person be appointed.
- Whether the appointment of the person with such a criminal history is likely to substantially conflict with STEPS's Values and the Code of Conduct or seriously erode public or customer confidence in STEPS.

The following factors may be taken into consideration in assessing any applicant's suitability for a position where a criminal record exists:

- **Nature of offence(s):** Any decision on employment should have regard to the relationship of the offence(s) to the role for which the applicant is being considered, including statutory and legislative requirements.
- **Number of offences:** Is there an established pattern of behaviour, which renders the applicant unsuitable for employment?
- **Severity of punishments:** The severity of the punishment imposed may be taken into account.
- **Age at which offences were committed:** The age at which offences were committed can be an important factor. Certain offences committed during youth may be viewed in an entirely different light to the same offences committed by a person of mature years.
- **Mitigating Circumstances:** Consideration should be given to anything mitigating or extenuating that might be revealed in relation to the offence(s) committed. These might include provocation, effect of alcohol and peer group pressure at the time of the offence and the circumstances in which the offence was committed.
- **General Character since the offences:** This aspect can have an important bearing in some cases, for example: steady employment record, and favourable reports from past employers.

5.1 NATURAL JUSTICE

When considering if an employee or applicant may be unsuitable for appointment or ongoing appointment, the employee/applicant must be provided with an opportunity to respond (natural justice).

The Responsible Officer or appropriate delegate will provide the applicant with:

- a copy of the criminal history report
- a request to confirm that they are the person to whom the criminal history report relates
- an invitation to make a written representation as to their suitability for appointment and to provide other information they consider may be relevant to the consideration of their circumstances and their suitability for appointment to STEPS.

The Responsible Officer is to act fairly, in good faith and without bias in considering the representations made by the applicant.

If there is no response to the request for the information above within the stipulated timeframe, no further opportunities will be provided.

5.2 RETENTION OF CRIMINAL HISTORY CHECKS

In ensuring compliance with the Information Privacy Act 2009, the criminal history provider FIT2WORK is the only authorised system to process, retain and store information relating to an employee’s identified criminal history.

The person requesting the criminal history check and/or human resources is not to record or store:

- information relating to an employee’s disclosable criminal history on an employee’s personnel file

- information relating to an employee's disclosable criminal history on the HR system, payroll system or other record keeping system
- any consent and/or criminal history application documentation.

The Working with Children Card and NDIS Worker Screening portals are the authorised systems for validation of these checks. Images of these cards are not to be recorded on HR, payroll systems or other record keeping system.

Working with Children Clearance (Ochre Card) (NT), NDIS Worker Screening Clearance (NT), Registration to Work with Vulnerable People (TAS), Registration to Work with Vulnerable People with NDIS Endorsement (TAS) and the superseded Yellow Card are the only Criminal History Checks to have images stored on the HR system. All expiry dates are to be stored on the HR system.

6.0 CHANGES TO CRIMINAL HISTORY

Where an employee's criminal history status changes, they are required to notify the Responsible Officer of any current and/or pending reportable activities (e.g. changes to their criminal record; charges before the courts; relevant investigations and/or work-related disciplinary procedures).

Employees are to notify the relevant authority of any activities that may affect an individual's ability to hold the relevant criminal history check.

Where such changes present a breach or potential breach of STEPS obligations under this procedure, the relevant ELT member and the Responsible Officer should conduct a criminal history assessment as outlined in paragraph 4.0.

7.0 POLICY EFFECTIVENESS AND ADHERENCE

The effectiveness of this policy will be assessed by monitoring the following:

- All STEPS employees hold all required criminal history checks
- Employees are completing the requirements of this procedure correctly
- Managers are monitoring employee compliance with this procedure.

Failure to adhere to the requirements of this procedure may result in disciplinary action up to and including termination of employment.

8.0 RELATED DOCUMENTS

Document Name	Document Name
Complying with the Australian Privacy Principles (i020700)	Disciplinary Action and Effective Termination (e210600)
Recruitment and Selection (e200100)	

9.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	7 April 2024
Effective Date	26 April 2024	**Document Number**	e200200_v8_240426

(Uncontrolled when printed)

ANNEXURE A

1. NDIS WORKER SCREENING CHECK REQUIREMENTS

STEPS employees in a Risk Assessed Role require a NDIS Worker Screening as provided by their relevant State or Territory legislation when:

- The employee is considered key personnel, as defined in S11A of the National Disability Insurance Scheme Act 2013 (for example, a CEO or a Board Member).

- The employee is engaged in the direct delivery of specified supports or services to a person with disability.

- The employee is likely to require 'more than incidental contact' with people with disability, which includes:

    - physically touching a person with disability

    - building a rapport with a person with disability as an integral and ordinary part of the performance of normal duties

    - having contact with multiple people with disability as part of the direct delivery of a specialist disability support or service, or in a specialist disability accommodation setting.

For the purposes of determining whether the normal duties of an employee will require more than incidental contact with a person with disability, contact includes physical contact, face-to-face contact, oral communication, written communication and electronic communication.

STEPS may, as a safety measure, require an employee performing a role outside of the conditions set above to have a NDIS Worker Screening.

Further information around the NDIS Worker Screening Requirements can be found under the National Disability Insurance Scheme (Practice Standards – Worker Screening) Rules 2018.

2. WORKING WITH CHILDREN CHECK REQUIREMENTS

STEPS will require all employees that meet the following conditions to undertake the relevant state or territory working with children check:

QUEENSLAND

If the employee meets ALL FIVE of the following conditions, you will need to get a Check:

- You are an adult engaged in work within the meaning of the Working with Children (Risk Management and Check) Act 2000 (QLD), which includes engaging in voluntary work and providing practical training as well as paid employment.

- You are working at or for one of the services, places or bodies, or in one of the activities listed in the Working with Children (Risk Management and Check) Act 2000 (QLD).

- Your work usually involves direct contact with a child or children. Direct contact means physical or face-to-face contact, or written (including postal), oral or electronic communication.
- The contact you have with children is not occasional direct contact and is not incidental to your work.
- You are not otherwise exempt from needing a Check under the Act.

NORTHERN TERRITORY

- A person is engaged in child-related employment if the person is engaged to perform child-related work.
- Child-related work is any work that involves, or may potentially involve, contact with children in connection with clauses 185.2 A through Q of the Care and Protection of Children Act 2007 (NT). Within the current scope of STEPS program delivery in the Northern Territory clause 185.2 B, education and care services.

TASMANIA

An employee who is taking part in a regulated activity with a vulnerable person (child) means contact that would reasonably be expected as a normal part of their role; and is one or more of the following:

- Physical contact including taking part in the regulated activity at the same place as the vulnerable person
- Oral communication, whether face-to-face or by telephone
- Written communication, including electronic communication.

Taking part in relation to a regulated activity includes, but is not limited to:

- Providing a service
- Being provided with a service
- Supervising, coaching or instructing a group or team
- Being a member of a group or team
- A person, although not taking part in the regulated activity, may meet or be in the immediate vicinity of a vulnerable person who is at the premises for the purpose of taking part in the regulated activity.

ANNEXURE B

A. STEPS CRIMINAL HISTORY CHECK MATRIX

	National police check	NDIS worker screening	Working with children check

Behaviour Support		☑	☑
Board & Executive Leadership Team	☑	☑	☑
Board Secretary	☑	☑	☑
Business Development	☑		
Business Management / Coordination	☑	☑	☑
Business Management / Coordination – NT	☑		☑
Casuarina Site – All Staff	☑		☑
Cleaners	☑		
Disability Employment Services	☑		☑
Education & Training	☑		
Education & Training – SEE / AMEP	☑		
Education & Training – Individual Support Trainers		☑	☑
General & Executive Management	☑	☑	☑
George St Site	☑		
Help Desk and Information Security			
Mental Health Programs (including CSTARS)		☑	☑
NDIS Services (including Work Mates and Behaviour Support)		☑	☑
Pathways – Boarding College		☑	
Pathways – Day Program		☑	☑
STEPS Pathways Charity	☑	☑	

STEPS Staffing Solutions	☑		
Volunteer Relationship Coordinator		☑	☑

APPLICATION PROCESS

To apply for your application/s, please refer to the below instructions for the state you are employed under. Please note STEPS pays the application fees for all Full Time and Part Time employees only. casual employees will need to pay for their applications due to the nature of their employment with STEPS.

NATIONAL POLICE CHECK

Upon commencement of your Employment with STEPS, if you are required to undertake a National Police Check, this will be issued to you at this time.

This process is renewed automatically via the FIT2WORK system every two years where employees will receive an invitation directly from FIT2WORK with the subject “Request to complete National Police Check - STEPS Group Australia” with instructions to undertake your renewal.

If your employment with STEPS at first did not require you to hold a National Police Check and now does require this check, you will be contacted by HR and then provided with the invitation to complete.

When the National Police Check returns from processing, HR will enter the details into the Human Resources Information System (HRIS).

NDIS WORKER SCREENING

For employees who require both the NDIS Worker Screening and Blue Card, you can apply for a combined application using the below instructions though you will need to tick Yes for any questions relating TO Working with Children.

The NDIS Worker Screening Check is conducted by the Worker Screening Unit in the state or territory where a person applies for it. The Worker Screening Unit also decides whether a person is cleared or excluded. Registered NDIS providers are required to ensure that they only engage workers who have been cleared in certain roles, called risk assessed roles.

How to apply in Queensland

If you would like to read the full instructions on how to apply, please click on the below link, otherwise refer to the steps below to get started. Before you start - Disability Worker Screening (communities.qld.gov.au)

Step 1: Have your customer reference number (CRN) ready

You will need a customer reference number (CRN) from Department of Transport and Main Roads (TMR) before you apply.

You can find this number on any product issued by TMR, such as:

- A driver’s licence
- Adult proof of age card

- Photo identity card
- Industry authority.

IMPORTANT: If you don't have a CRN, or **if your photo was taken more than 5 years and 3 months ago**, you will need to visit a TMR service centre to update your photo.

For further information on how to get a CRN please see the Identity verification fact sheet.

Step 2: Register for an online account and commence your application

Firstly: To register an online account, click - QLD Disability Worker Screening (communities.qld.gov.au)

Secondly: Once you have registered for your online account, you **must** log in to the online worker portal to apply for your card. Click - QLD Disability Worker Screening (communities.qld.gov.au)

IMPORTANT: When it comes to the payment section select that your **employer (STEPS Group Australia) will be paying on your behalf** and enter the HR@stepsgroup.com.au email so that HR receives the request to pay for your application.

If you have already registered for an online account, you can login to your worker portal to commence a new application (or combined application with blue card), update an existing application, or check on the progress of a submitted application.

Note: The online application works best using current browsers such as Chrome, Firefox, Safari or Edge. There may be compatibility issues with older browsers such as Internet Explorer 11 or earlier.

When you receive your NDIS Worker Screening Clearance, please enter the details into the Human Resources Information System (HRIS).

How to apply in Tasmania

Before applying for NDIS worker screening, you first must apply for a registration to work with children with a NDIS endorsement. To get this endorsement, your NDIS employer (this includes a NDIS participant) must verify your work. Your application will NOT proceed without this verification. You will need to provide your employer details so have this information ready before starting your application. Further instructions are provided when you apply.

Please follow the below instructions to obtain a registration to work with children with a NDIS endorsement.

You will need to have the following information ready:

- your previous names and/or alias
- an email address and/or mobile number
- the address of every place you have lived over the last five years (including dates you lived at the addresses)
- evidence to prove your identity

- details for each organisation you will be working or volunteering for including the name, address, contact person, phone number and email address
- if you have lived outside of Australia for 1 year or more, you will need to provide dates
- details of any overseas offence history
- details of any family violence orders, restraint orders, apprehended violence orders (taken out against you)
- details of any child protection orders you have been involved in.

Complete the online application form

- if you get paid for your role, select **Employment/Volunteer**
- if you are a volunteer and do not get paid, receive material benefit or reward, select **Volunteer**
- print the application receipt or write down your reference number
- pay the application fee (online by credit card) or at any Service Tasmania shop (external link) to:
  - have your photo taken
  - pay the application fee if you haven't already paid online
  - accept the Terms and Conditions if someone has filled out the form on your behalf.

To apply from interstate or overseas, see interstate and overseas applicants.

Your application will not begin processing until you have completed the steps above.

Please note that the application fee is non-refundable.

When you receive your NDIS Worker Screening Clearance, please enter the details into the Human Resources Information System (HRIS).

WORKING WITH CHILDREN CHECK

How to apply in Queensland

You will need a Customer Reference Number (CRN) from the Queensland Department of Transport and Main Roads (TMR) before you apply for your blue or exemption card to prove your identity. You can find your CRN on any TMR product.

If you don't have a CRN, or your photo has expired, you will need to visit a TMR customer service centre to obtain one. If you are unable to visit TMR or live interstate you can still apply for a CRN. There is no fee to get a CRN or have your photo updated.

To apply for a blue or exemption card, follow these 3 steps.

1. Have your CRN nearby to reference
2. Register for an online account. This is how the Department verifies your identity and obtains the photo for your card

3. Apply for your blue or exemption card using the online applicant portal.

IMPORTANT: When it comes to the payment section, please contact the HR team on 07 5458 3096 to arrange payment. You will then be provided with a receipt number to finalise your application.

When you receive your Working with Children Clearance, please enter the details into the Human Resources Information System (HRIS).

How to apply in the Northern Territory

You must complete the online application for a working with children clearance in one sitting.

You can't save your information and return to it.

You will need all of the following ready:

- a debit or credit card - MasterCard or Visa only
- an email address
- an Australian residential and postal address
- scanned copies of your identity documents, a passport-sized photo and, if you are a volunteer, a completed volunteer concession form to pay the reduced fee.

Provide your scanned documents in GIF, JPG, PDF, PNG or TIFF format.

When you receive your Working with Children Clearance, please enter the details into the Human Resources Information System (HRIS).

How to apply in Tasmania

Before you start your application, you will need to have the following information ready:

- your previous names and/or alias
- an email address and/or mobile number
- the address of every place you have lived over the last five years (including dates you lived at the addresses)
- evidence to prove your identity
- details for each organisation you will be working or volunteering for including the name, address, contact person, phone number and email address
- if you have lived outside of Australia for 1 year or more, you will need to provide dates
- details of any overseas offence history
- details of any family violence orders, restraint orders, apprehended violence orders (taken out against you)
- details of any child protection orders you have been involved in.

Complete the online application form

- if you get paid for your role, select **Employment/Volunteer**
- if you are a volunteer and do not get paid, receive material benefit or reward, select **Volunteer.**
- print the application receipt or write down you reference number
- pay the application fee (online by credit card) or at any Service Tasmania shop (external link) to:
    - have your photo taken.
    - pay the application fee if you haven't already paid online.
    - accept the Terms and Conditions if someone has filled out the form on your behalf.

To apply from interstate or overseas, see interstate and overseas applicants.

Your application will not begin processing until you have completed the steps above.

Please note that the application fee is non-refundable.

When you receive your Working with Children Clearance, please enter the details into the Human Resources Information System (HRIS).

NATIONAL POLICE CHECK

You will receive an email from our National Police Check provider Fit2Work from Equifax. This email will provide you with a step-by-step guide on how to complete your check.

1.4.4 Disciplinary Action and Effective Termination

1.0 INTRODUCTION

The purpose of this procedure is to provide guidance on disciplinary action and managing termination effectively and to be compliant with the provisions of relevant legislation and workplace agreements and that all employees have access to a fair and equitable process in the event of disciplinary action or termination.

1.1 DEFINITIONS

National Employment Standards	The *National Employment Standards* are ten (10) minimum employment entitlements provided to all employees
Termination	**Termination** of employment is when an employee’s contract of employment with STEPS ends. This may happen due to redundancy, resignation or dismissal.

2.0 PRINCIPLES

- STEPS will endeavour to give an employee the opportunity to fix any performance issues using Disciplinary Action or Warnings. The Executive Manager - Human Resources can provide further information and advice regarding this course of action.

- STEPS’ effective termination of an employee aspires to be in line with the *Fair Work Act 2009 (Cth)* and the *National Employment Sta*ndards, along with any applicable employment contract or enterprise agreement.
- As per STEPS’ Anti-Discrimination and Equal Employment Opportunity Policy (i010102), equity and diversity principles and practice underpin decision making, daily operation and management of professional relationships.

2.1 PROHIBITED REASONS FOR DISMISSAL

- The *Fair Work Act 2009* prohibits dismissal, or other adverse action, on the following grounds:
  - Temporary absence from work because of illness or injury;
  - Union membership or participation in union activities outside working hours or, with the employer's consent, during working hours;
  - Non-membership of a trade union;
  - Seeking office as, or acting or having acted in the capacity of, a representative of employees;
  - The filing of a complaint, or participation in proceedings, against an employer involving alleged violation of laws or regulations or recourse to competent administrative authorities;
  - Race, colour, sex, sexual preference, age, physical or mental disability, marital status, family or carer’s responsibilities, pregnancy, religion, political opinion, national extraction or social origin; (except in certain circumstances)
  - Absence from work during maternity or other parental leave; and,
  - Temporary absence from work because of the carrying out of a voluntary emergency management activity, where the absence is reasonable having regard to all the circumstances.
- Any dismissal which contravenes any of the above prohibited grounds constitutes “unlawful” termination of employment.
- In considering whether a dismissal is harsh, unjust or unreasonable, the following will be taken into account:
  - Whether there was a valid reason for the dismissal related to the employee’s capacity or conduct
  - Whether the employee was notified of that reason and given an opportunity to respond
  - Any unreasonable refusal by the employer to allow the employee to have a support person present to assist at any discussions relating to dismissal
  - If the dismissal related to unsatisfactory performance by the employee, whether they had been warned about that unsatisfactory performance before the dismissal
  - The degree to which the size of the employer’s enterprise and the degree to which the absence of dedicated human resource management specialists or expertise would be likely to impact on the procedures followed in effecting the dismissal
  - Any other matters that the Fair Work Commission considers relevant.
- Dismissal of an employee must be in line with the STEPS’ Delegations Register (i010601).

2.2 DISCIPLINARY ACTION

- Where an employee displays misconduct (see below in 2.2.1) that warrants disciplinary action they will be given a written warning detailing:
    a) Details of the required standards for conduct and how the employee has failed to meet those standards.
    b) Details of any assistance measures agreed to with the manager.
    c) Details of how the employee's conduct will be assessed/monitored and over what time period.
    d) The possible consequences if the employee displays similar misconduct within the specified time period, and
    e) That the employee is requested to respond within 72 hours (either in writing, or at a meeting, where a support person may be present) with any relevant information.
- At the end of the specified time period if the employee's conduct is assessed as meeting the required standard no further action need be taken under these provisions. All documentation will be retained on the employee's personal file.
- If the employee's conduct does not meet the required standard, the manager/supervisor will report this to the relevant business stream Executive Leadership Team member for discussion and approval of action. The manager/supervisor will advise the employee of the action to be taken, which may include one or more of the following:
    - Termination of employment.
    - move to lower classification.
    - Reassignment of duties; and/or
    - Some other appropriate action
- The employee will be given a minimum of twenty-four (24) hours from the receipt of the advice to respond to the findings and the action proposed.
- The relevant business stream Executive Leadership Team member, having taken into account the manager/supervisor's findings and the employee's response, will advise the employee in writing of the final decision.
- In exceptional cases, STEPS reserves the right to dispense with some or all of these stages of the procedure.

2.2.1 MISCONDUCT

Misconduct may include any of the following, but is not limited to:

- A breach of the Code of Conduct and Ethical Behaviour (e210007).
- Any wilful breach of any STEPS' policy.
- Harassment or coercion of another employee.
- Serious, wilful negligence or carelessness in the performance of duties or failure to perform duties assigned.
- Any act or failure to act that has the possibility of damaging the reputation of STEPS.
- Knowingly use of a substance including alcohol or a drug that results in impaired performance or improper conduct at the place of employment.
- Knowingly provide false or misleading information to STEPS in respect of an application for appointment or promotion, or in the course of employment.

  - Failure to remedy previous misconduct or failure to comply with former counselling or admonishment; and
  - Deliberate or reckless damage to or destruction of employer property or equipment.

3.0 TERMINATION PROCEDURE

3.1 DEATH OF AN EMPLOYEE

- Upon receipt of legal authority and details from the person handling the deceased estate, the Human Resources Team will calculate and pay any outstanding salary and leave entitlements as from the last known working day.

3.2 ABANDONMENT OF EMPLOYMENT

- The absence of an employee from work for a continuous period exceeding three (3) working days without the consent of the employer and without notification to the employer may be evidence that the employee has abandoned their employment.
- The Manager/Supervisor will undertake reasonable efforts to contact the employee, including making immediate contact with the provided Emergency Contact person (within 24 hours) on ConnX, communication sent via registered mail to employee's home address, email with 'delivered' and 'read' receipts. Correspondence will raise concern about the employee's absence and advise that if there is no response within a reasonable timeframe (usually about one week), STEPS will consider that the employee has abandoned their employment.
- The employee will be provided with the opportunity to make contact and explain their absence. Sometimes what appears to be abandonment can either be absence due to a serious illness or accident or just a misunderstanding.
- If within a period of fourteen (14) working days (or less, dependent upon the relevant Award or Agreement) from an employee's last attendance at work (or from the date of their absence where notification was given or consent granted) an employee has not established to the satisfaction of the relevant business stream Executive Leadership Team member that they were absent with reasonable cause, the employee will be deemed to have abandoned their employment and will be terminated.
- Where an employee has abandoned their employment, all pay and other benefits provided under their employment arrangement will cease to be available until the employee resumes work, or is granted leave. The period of absence will not count as service for any purpose.
- Where an employee is terminated by abandonment, the employee will not be entitled to notice of termination or payment in lieu of notice.

3.3 TERMINATION DUE TO UNDER PERFORMANCE

- The Managing Underperformance Procedure (e230300) will apply prior to a decision to terminate employment on the grounds of underperformance.
- If the Manager/Supervisor has deemed the completion of the Performance Improvement Plan (e220301) unsuccessful and there has been inadequate improvement and/or non-participation, the employee is advised that their continued employment will be reviewed and may be subject to termination. The employee is advised that they may bring a support person if they choose. However, the employee does not have the right to use a solicitor or other legal representative at the meeting. A witness / scribe may be present to listen and assist the Manager/Supervisor in note taking.

- The employee will be given a minimum of twenty-four (24) hours) to respond to the underperformance concerns as outlined in the Performance Improvement Plan and the letter advising their continued employment will be reviewed and may be terminated. No decision on what may be an appropriate response has been made or will be made prior to receipt of the employee's response and evaluation by management.
- Upon receipt of the employee's response, the Manager/Supervisor will make a determination in relation to continuation of employment and provide evidence to seek support from the relevant business stream Executive Leadership Team member to terminate due to an employee's under performance.
- STEPS may also consider whether there is a case for alternative employment which the employee may be capable of performing.
- The offer of alternative employment will be at the sole discretion of the Manager/Supervisor and this will be approved by the relevant business stream Executive Leadership Team member and offered to the employee at the dismissal meeting, whereby the employee may be given reasonable time to consider the offer.
- The termination letter provided to the employee is prepared by Human Resources.
- In exceptional cases, STEPS reserves the right to dispense with some or all of these stages of the procedure.

3.4 TERMINATION OF PROBATIONARY EMPLOYMENT

- If at any time during the probationary period an employee's conduct is considered to be unsatisfactory or the employee is not satisfied with the position, either the employee or STEPS may terminate the employment subject to giving termination notice as per the Probation Procedure (e220100).

3.5 TERMINATION DUE TO SERIOUS MISCONDUCT

- Conduct by an employee that is intentional and causes serious immediate risk to the health or safety of a person, or the reputation, viability or profitability of the business is considered serious misconduct. Serious misconduct includes both of the following:
  - Wilful or deliberate behaviour by an employee that is inconsistent with the continuation of the contract of employment;
  - Conduct that causes serious and imminent risk to:
    a) the health or safety of a person; or

    b) The reputation, viability or profitability of the employer's business.
- Conduct that is serious misconduct also includes each of the following:
  - The employee, in the course of the employee's employment, engaging in theft; or fraud; or assault; or abuse, neglect and exploitation;
  - Or the employee being intoxicated at work;
  - The employee refusing to carry out a lawful and reasonable instruction that is consistent with the employee's contract of employment.
- In circumstances where STEPS has reasonable course to believe an employee has committed an act of serious misconduct, the employee will be notified in writing and will be expected to

respond thereto within 24 hours of the notice and during such time the employee may be suspended on full pay.

- Where an employee has been found to have committed any act of serious misconduct, the employee may have their employment terminated with immediate effect. Depending on the nature of the misconduct the Police and/or the NDIS Commission may need to be informed.

- STEPS may terminate without notice the employment of an employee found to have engaged in serious misconduct such that would make it unreasonable to require STEPS to continue employment during a period of notice.

3.6 TERMINATION ON THE GROUNDS OF ILL HEALTH

- There are significant constraints on the employer’s ability to terminate for reasons such as disability or short term illness. Some of the constraints are summarised below:

Medical Issue	Constraints
Short term illness or injury	Employees are entitled to access paid leave. Unlawful to terminate due to illness or injury where the absence is less than three months in a twelve month period, in addition to paid leave entitlements.
Work related injury	It is generally unlawful to terminate employment where the employee is in receipt of Workers Compensation, for periods of between 6 and 12 months. Advice to be sought from the Executive Manager - Human Resources
Chronic illness, disability	Anti-discrimination and equal opportunity legislation in both state and federal jurisdictions generally impose an obligation on employers to make reasonable accommodation for disability

- STEPS management may require an employee whose absence extends for more than three (3) months or the total absences of the employee, within a twelve (12) month period, have been more than three (3) months (whether based on a single illness or injury or separate illnesses or injuries) to undergo a medical examination by a specialist medical practitioner chosen by STEPS at the expense of STEPS.
- STEPS management may require an employee, whose capacity to perform the inherent duties of their position is in doubt, to undergo a medical examination by a specialist medical practitioner chosen by STEPS at the expense of STEPS.
- The Manager will provide the employee with written notice of not less than thirty (30) days that a specialist medical examination is required.
- Failure to undergo a specialist medical examination within thirty (30) days of a written notification to do so will be taken as evidence that the employee is unable to perform assigned duties.
- A specialist medical examination will not be required if an employee elects to apply to the relevant superannuation fund for ill-health retirement or temporary disability benefit and is granted the benefit.

- STEPS will consult with the employee to better understand their circumstances and how best to manage their situation with regard to superannuation benefits.
- Where the superannuation fund determines that an employee is ineligible because of a pre-existing medical condition, or decides that an employee following a period of receipt of a temporary disability benefit, is capable of resuming work and the Manager/Supervisor elects the dispute of this decision, the Manager/Supervisor may proceed to request the employee undergo a specialist medical examination.
- A copy of the medical report made by the specialist medical practitioner will be made available to the Manager/Supervisor.
- A copy of the medical report made by the specialist medical practitioner may be obtained by the employee through their personal medical practitioner.
- The medical report should advise the likely timeframe within which the employee's capacity might improve, whether there are any specific restrictions which might apply upon a return to work, whether modifications to the role might assist, or whether the employee might be fit for other duties.
- It is only after obtaining objective medical evidence and providing the employee with an opportunity to respond to the findings that a decision should be made. Options could include a return to work, possibly with some temporary or permanent modifications to duties, transfer to more suitable duties, or termination of employment.
- In instances where the STEPS decides to terminate employment on the grounds of ill health, termination notice will be in aligned to the *National Employment Standards* (NES).
- Where the superannuation fund determines that an employee is totally and permanently incapacitated and is unlikely to return to work in the foreseeable future, STEPS may terminate the employment.
- In exceptional cases, STEPS reserves the right to dispense with some or all of these stages of the procedure.

3.7 REDUNDANCY

- When the Managing Director is aware that an employee's position is likely to become excess to the needs of the organisation:
  - The Managing Director will take all reasonable steps, consistent with the efficient management of the department, to assign the employee to a suitable vacancy; and
  - The Managing Director (or delegate) will at the earliest practicable time advise the employee.
- The Managing Director (or delegate) will not advise an employee that their position is excess until discussions have been held with the employee to consider redeployment opportunities, including whether the employee seeks redeployment, whether voluntary redundancy may be appropriate and whether the employee wants to be offered voluntary redundancy. The employee may be accompanied by a person of their choice to provide support.

3.8 EXEMPTIONS

- Consistent with Industrial Relations law, no written warnings are required to be issued to casual staff (under 12 months of service), volunteers, or employees employed in an independent contractor arrangement. If found to be in breach of the Code of Conduct and Ethical Behaviour (e210007) or unsatisfactory performance, subsequent decisions on disciplinary action will be at the discretion of the Manager/Supervisor, dependent on the seriousness of the infraction.

- It is recommended that a conversation occurs with the casual, volunteer, or employee employed in an independent contractor arrangement to advise that their employment has been terminated and the reasons for this.

4.0 REFERENCES

Fair Work Act 2009 (Cth), Part 3-2 Unfair Dismissal

National Employment Standards

5.0 RELATED DOCUMENTS

Document Name	Document Name
Anti-Discrimination and Equal Employment Opportunity Policy (i010102)	Code of Conduct and Ethical Behaviour (e210007)
Delegations Register (i010601)	Letter – Written Warning (HR Only)
Letter – Termination (HR Only)	Managing Underperformance Procedure (e230300)
Performance Improvement Plan (e220301)	Probation Procedure (e220100)

6.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	1 November 2024
Effective Date	7 November 2024	**Document Number**	e210600_v3_241107

(Uncontrolled when printed)

1.4.5 Displaying Personal Pronouns in Email Signature Blocks

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) views the inclusion of personal pronouns in email signatures as a concrete step towards creating an inclusive culture. This practice aligns with the company's values of Integrity, Courage, Respect, and Understanding, and demonstrates a commitment to creating a safe, respectful, and diverse workplace environment.

1.1 DEFINITIONS

Personal Pronoun	A personal pronoun is a pronoun typically used to refer to a speaker or to the people or things that a speaker is referring to. Often, personal pronouns are used to replace proper names as in Olivia went to bed early because she (Olivia) worked hard today.

2.0 PURPOSE

To create an inclusive workplace environment by allowing employees to display their personal pronouns in their email signature blocks, thus fostering a culture of respect and understanding. This procedure outlines the process for opting in, modifying, or opting out of displaying personal pronouns, as well as the responsibilities of Human Resources (HR) and Information and Communications Technology (ICT) in this regard.

3.0 SUPPORTED PRONOUNS

Employees can choose from the following pronoun options:

- She/Her
- He/Him
- They/Them
- Name/Name (for those who prefer to be identified by their name rather than gender-relative pronouns)
- Employees can also use self-described pronouns, which will be reviewed by HR. If necessary, a HR representative will contact the employee for further discussion.

3.1 SECONDARY PRONOUNS

Both new and existing employees can specify secondary pronouns if required.

4.0 PROCESS

4.1 OPTING IN

- New employees: During the onboarding process, new employees will have the opportunity to opt in and provide their preferred personal pronouns.
- Existing employees: Current employees can opt in by accessing the "Personal Pronouns" section of the HR page on the Staff Information Destination (SID).

4.2 MODIFYING PERSONAL PRONOUNS OR OPTING OUT

- **Modifying Pronouns:** Employees can update their personal pronouns via the "Personal Pronouns" section on the HR page in SID.
- **Opting Out:** Employees who wish to opt out of displaying personal pronouns should send an email to HR at HR@stepsgroup.com.au expressing their request.

5.0 RESPONSIBILITIES

HR is responsible for collecting employees' personal pronoun preferences, facilitating changes, and addressing related queries.

It is ICT's responsibility for integrating the personal pronoun information into employee email signature blocks.

Personal pronouns should be reflected in employees' email signature blocks within two weeks of their commencement or opt-in date.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Anti-Discrimination and Equal Employment Opportunity Policy (i010102)	Diversity and Inclusion Policy (i010102)
Workplace Bullying and Harassment Policy (i010105)	Preventing and Responding to Bullying and Harassment (i050700)

7.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	2 November 2023
Effective Date	7 November 2023	**Document Number**	i052800_v1_231107

(Uncontrolled when printed)

1.4.6 Dress Standards

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to presenting a consistent, professional image to customers, stakeholders, and the general community. How employees dress reflects STEPS and its culture. As representatives of STEPS, it is important for all employees to uphold the dress standards.

1.1 RESPONSIBILITIES

Managers must:

- Ensure employees adhere to professional presentation standards in line with this procedure at all times

- Ensure the consistent role modelling and application of this procedure
- Make appropriate decisions where specific requirements and/or exceptions will apply under this procedure (see below)

Employees must:

- Adhere to a professional presentation standard in line with this procedure at all times while representing STEPS
- Dress neatly and appropriately for the type of work they perform
- Ensure that work attire is kept clean and presentable at all times
- Not wear STEPS branded attire to social functions which do not form part of the employee's duties.

2.0 DRESS STANDARDS

STEPS expects all employees to wear clothing which meets a presentable standard for their particular workplace, suits their relevant working environment and complies with Work Health and Safety (WHS) standards.

The following dress codes always apply:

- All employees must be always well-groomed.
- All clothes must be workplace appropriate and respectful. (e.g., In the office, wear office appropriate attire).
- All clothes must project professionalism.
- All clothes must be clean and in good condition. Visible stains, rips, tears or holes are not acceptable.
- Collared shirts, such as polo shirts, are deemed appropriate.
- Denim is not considered to be appropriate office attire.
- Activewear and other clothing typically worn for leisure activities are not acceptable.
- Clothes which are revealing or inappropriate are not acceptable (such as clothing that reveals the midriff, cleavage or bare shoulders).
- Employees are to avoid wearing clothes with words or images which may offend others.

3.0 PERSONAL HYGIENE

All employees must always maintain a high standard of personal hygiene.

4.0 FOOTWEAR

Footwear must be appropriate for the task performed and suitable for the floor surfaces where the work is being conducted. Where specific requirements exist, these will be advised by the employee's Manager and in the Safe Work Procedures/Job Safety Environmental Analysis (JSEA). Safe footwear does not include thongs, slides, shoes without a backstrap, slip on sandals, crocs. Sneakers are only permitted if approved by your site manager.

5.0 STEPS BRANDED WORKWEAR

Generally, STEPS does not require employees to wear a uniform, however, all full time and part time employees will be provided with one STEPS branded polo shirt with the logo at no cost to the employee. Employees will be able to purchase additional shirts at their own expense.

6.0 RESPONSIBILITIES WHEN WEARING STEPS BRANDING

Where an employee is identifiable by STEPS branding outside the performance of their duties, they should conduct themselves in a way that is consistent with the Code of Conduct and Ethical Behaviour (e210007) and relevant policies and procedures.

7.0 SPECIFIC REQUIREMENTS

Certain staff members may be required to meet special dress, grooming and hygiene standards, such as wearing uniforms or protective clothing, depending on the nature of their job. On these occasions, STEPS employees are still expected to present a neat appearance, and are not permitted to wear ripped, frayed, or dishevelled clothing.

8.0 EMPLOYEE IDENTIFICATION

In certain circumstances, employees should have a name badge or lanyard to identify them as a STEPS employee. For example:

- Attending official events and functions as a STEPS representative, including meetings, conferences, seminars, and networking events
- Meeting external stakeholders (e.g., consultants, clients, suppliers, etc)
- Name badges/lanyards will feature the STEPS logo. Employee identification must be kept clean and in good condition.

9.0 ACCESSORIES & BODY ART

- Jewellery should be appropriate to the employee’s work environment and meet any required WHS standards.
- All tattoos which could be perceived as offensive are to be discreetly covered where possible.

10.0 CASUAL DRESS DAYS

At various times there may be STEPS approved ‘casual’ or ‘dress down’ days. The standards outlined in this procedure will still apply on those days. Casual dress day will not apply if employees are meeting with clients, or other external stakeholders.

11.0 EXCEPTIONS

STEPS promotes diversity in its workforce and therefore, nothing within this procedure is intended to prevent an employee wearing religious or cultural dress, unless it presents a WHS risk and an alternative control for that risk cannot be implemented.

As an Equal Opportunity Employer, STEPS understands that flexibility may be required in the event that certain circumstances prevent an employee from complying with this procedure. Where genuine hardship or particular operational needs warrant, one-off exceptions may be made on a case-by-case basis; please discuss in the first instance with the Manager or Human Resources.

12.0 RELATED DOCUMENTS

Document Name	
Code of Conduct and Ethical Behaviour (e210007)	STEPS Staff Polo Top and Badge Order Form (office.com)

13.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	19 June 2023
Effective Date	20 June 2023	**Document Number**	e200300_v3_230609

Uncontrolled when printed)

1.4.7 Drugs and Alcohol in the Workplace

1.0 DRUGS AND ALCOHOL IN THE WORKPLACE

This procedure outlines the process for dealing with drugs and alcohol in STEPS Group of Companies (STEPS) workplaces.

1.1 DEFINITIONS

Authorised Doctor	Any registered medical practitioner authorised by STEPS.
Drugs of Abuse	A legal drug, misused prescription drug or illegal drug that could impair a worker's operation of a vehicle, plant, equipment, or client care in the performance of a worker's duties
Illegal Drug	Any drug which is unlawful to possess, consume or sell within the Commonwealth of Australia or in any individual state of Australia.
Misused prescription drugs	Prescription drugs used incorrectly when compared with the prescription given by a registered medical practitioner.
Legal Drugs	Substances that may lawfully be taken without a prescription from a registered medical practitioner (for example, nicotine, caffeine, alcohol) or prescription medications provided they have been prescribed by a registered medical practitioner.
Impaired	A documented or observed decrease in the performance and outcome indicators of a worker's duties.
Equipment	Any plant or equipment that is owned and/or operated by STEPS or being used by worker's to perform duties for the organisation.

Suspicion	Suspecting, on reasonable grounds, that a worker's performance and outcomes are impaired by the use of drugs of abuse or alcohol and/or that a work incident has been totally of partially as a result of the use of alcohol or drugs of abuse and the worker is in breach of the Fitness for Work Policy (i010104)
PRESCRIBED LIMITS	
Zero tolerance	0.00 blood alcohol (BAC) as determined by an accurate alcometer.
Illegal Drugs	Levels of illegal drugs in a collected urine sample not exceeding the cut-off levels as stated in ASNZS 4308:2008 and determined by GC-MS and LC-MS confirmatory testing.
Prescription Drugs	Levels of prescribed drugs in a collected urine sample defined as being within therapeutic levels and not recreational levels as stated in ASNZS 4308:2008 and determined by GC-MS and LC-MS confirmatory testing.
Legal Drugs	A level up to but not exceeding: the cut-off level identified in ASNZS 4308:2008; or the permissible quantity if the substance were used strictly in accordance with either the manufacturer's recommended dosage rate or the prescription given by a registered medical practitioner (caffeine, nicotine are not tested for because they are not considered to be a drugs of abuse).

1.2 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Ensure that this procedure is embedded into the daily STEPS operations.
- Make appropriate decisions where exceptions will apply under this procedure.

Supervisors will:

- Role model the application of this procedure at all times.
- Ensure that all employees are made aware and understand this procedure on commencement, as part of their Induction and at regular intervals of their employment.
- Observe the behaviour of employees to ensure adherence with the procedure.
- Observe employee performance indicators and outcomes to ensure that KPIs are being met.
- Identify any performance and safety concerns or issues and address them proactively and expediently to ensure the health and safety of all workers.
- Subject to any disclosures required by law, treat any notifications received confidentially.
- Ensure support is provided to employees where appropriate.
- Manage any suspected breaches of this procedure by acting promptly and in accordance with this procedure and the *Performance Management and Disciplinary Matters Procedure* (under construction).

Employees will:

- Comply with this procedure.
- Observe all directions from their supervisor or ELT member in regard to this procedure.
- Recognise that their performance of duties could be affected by alcohol or drugs.
- Immediately notify their supervisor if they are aware of any breach of this procedure by another employee.
- Immediately notify their supervisor if they receive a gift of alcohol or if they carry alcohol or a drug of abuse while attending any STEPS workplace and, if required, immediately remove it from site.
- Recognise that a failure to report any breach of this policy by another employee may itself be considered a breach of this procedure.

2.0 DRUGS AND ALCOHOL PROHIBITION

The governing organisational policy on drugs and alcohol in STEPS workplaces is:

- STEPS will not tolerate an employee's consumption of alcohol and/or illegal drugs and/or misuse of prescription drugs while at work.
- Having a blood alcohol content greater than 0.00 while operating STEPS vehicles or equipment at any STEPS workplace.
- Having levels of illegal drugs in a collected urine sample that exceed the cut-off levels as stated in ASNZS 4308:2008 and determined by GC-MS and LC-MS confirmatory testing while operating STEPS vehicles or equipment or while performing their duties at any STEPS workplace.
- Having levels of prescribed drugs in a collected urine sample that exceed therapeutic levels as stated in ASNZS 4308:2008 and determined by GC-MS and LC-MS confirmatory testing while operating STEPS vehicles or equipment or while performing their duties at any STEPS workplace.
- Any employee suspected of having a blood content greater than 0.00 while operating a STEPS vehicle, plant, or equipment, or being impaired by alcohol and/or illegal drugs and/or misuse of prescription drugs will be subject to testing.
- The illegal or unauthorised possession, consumption, or sale of alcohol and/or drugs of abuse whilst attending any STEPS workplace is prohibited.
- Any employee found to be impaired by a process of drug and alcohol testing or found to be in possession of undeclared alcohol and/or drugs of abuse at the workplace will be managed through a disciplinary process, up to and including termination of employment.

Employees, who are employed in a remote community in Australia that has restrictions in place for the purchase and consumption of alcohol, must abide by these restrictions whilst they are working in that location.

When an employee is suspected of being impaired in the workplace, STEPS primary consideration will be for the safety of the individual, other employees, and clients in the workplace.

STEPS will undertake testing for alcohol and/or drugs of abuse when an employee is under suspicion:

- When a employees performance is suspected of being impaired as a result of:

    - Observed incorrect behaviours.
    - A documented decrease in performance indicators or outcomes.
- When an employee demonstrates signs of being impaired by alcohol and/or drugs of abuse.
- When a work incident is suspected to be as a result of an employees consumption of alcohol and/or drugs of abuse.

3.0 PRESCRIPTION AND PHARMACY DRUGS

Where an employee is taking prescription or pharmacy drugs for medical purposes, the employee will not breach this procedure by attending work, if the employee:

- Takes the prescription and pharmacy drugs in accordance with the instructions of their medical practitioner and normal directions applying to the use of those drugs.
- Does not misuse or abuse the use of prescription or pharmacy drugs.
- Ensures they are able to perform their work effectively, competently, and safely.
- Ensures they are informed of the impact of consumption of alcohol with prescription and pharmacy drugs and they limit consumption accordingly.
- The drug of abuse does not affect the employees ability to operate STEPS vehicles, machinery and equipment and safely perform their normal work duties.

If an employees ability to perform work competently, efficiently, and safely is affected, the employee should obtain this advice in writing from the medical practitioner, or pharmacist, and provide it to their supervisor as soon as possible and before undertaking their work.

If a supervisor observes changes in the employees ability to safely perform, taking into consideration performance indicators and outcomes, they must document this change and take steps to address the issue in accordance with this procedure.

4.0 DRIVING STEPS VEHICLES AND OPERATING STEPS EQUIPMENT

Alcohol and drugs of abuse

Employees must comply with prescribed limits applicable to particular duties they perform, or may be called on to perform, at all times. STEPS' vehicles, plant and equipment are not to be operated by an employee if their BAC is greater than 0.00 or if a worker’s consumption of drugs of abuse is greater than prescribed limits.

STEPS will not accept liability for any damage to a STEPS vehicle, plant and equipment, an injury to another person, or damage to other property caused by an employee if drug and alcohol testing confirms the presence of alcohol and drugs of abuse at levels greater than prescribed limits. The employee will be held personally liable in such circumstances.

5.0 WHERE AN EMPLOYEE IS SUSPECTED TO BE UNDER THE INFLUENCE OF DRUGS OR ALCOHOL

If a supervisor suspects, on reasonable grounds, that an employee is under the influence of drugs or alcohol and in breach of the Fitness for Work Policy (i010104), the supervisor will take steps to address the issue. Reasonable grounds may include (but are not limited to) where the employee:

- Is observed to display incorrect behaviours in the workplace including:
    - Being unable to coordinate their actions.

    - Has red or bloodshot eyes, or dilated pupils.
    - Smells of alcohol.
    - Acts contrary to their normal behaviour.
    - Is not behaving in a professional and competent manner and in accordance with behavioural expectations.
- Appears to be impaired or affected by alcohol or drugs.
- Is involved in a traffic accident that appears to have been influenced by the consumption of alcohol or drugs.
- Is observed to have a negative change in performance indicators and outcomes and this has been documented.

In such circumstances, the supervisor may take the following immediate actions (but is not limited to these actions):

- Initiate either a breath alcohol test and/or oral fluid sample to be completed by an appropriately trained, nominated external testing provider.
- Stand the employee down from duties until assessment of the testing results can be undertaken.
- Arrange transport home for the employee.
- Obtain statements from co-workers to assist the supervisor with their assessment, ensuring strict confidentiality will be maintained during the collection of such statements.

In the case of prescription or pharmacy drugs, the supervisor may request evidence in relation to the effects and proper use of the drug.

STEPS will ensure:

- Testing and assessment with the nominated external testing provider is organised to be undertaken at the earliest possible opportunity.
- Information on the nominated external testing provider’s procedures is provided to the employee at the time of the testing.
- Australian Standards (AS 4760:2006, ASNZS 4308:2008 and AS ISO 15189:2013) will be followed by the providers and their affiliates for the collection and handling of biological samples.
- All test results are assessed by an Authorised Doctor, in conjunction with taking a medical history and assessment of the affected employees.

Employees must:

- Attend the appointed testing and assessment times.
- Contact their supervisor to confirm that they have attended the appointments, as directed.
- Not refuse testing or fail to provide adequate information during testing.

Refusal to attend a medical examination or drug and alcohol testing, refusal to go home, or providing false information constitutes a breach of these procedures and may result in disciplinary action being taken against the employee.

6.0 WHERE DRUGS OR ALCOHOL IS FOUND IN THE WORKPLACE

Where drugs or alcohol is found at the workplace in breach of these procedures, or it is suspected that an employee has drugs or alcohol in their possession at work, their supervisor may take the following action, which includes, but is not limited to:

- Investigating the matter to attempt to determine whether the employee does have such drugs or alcohol in their possession.
- Requesting employees to provide access to bags, workspace areas, lockers, or vehicles, or to empty their pockets or jacket for the purpose of locating any drugs or alcohol.
- Requiring employees to undergo testing for the presence of drugs or alcohol.

Employees are required to co-operate in any investigation or inspection process.

7.0 WORK RELATED FUNCTIONS

The consumption of alcohol is not permitted at work events. However, STEPS recognise that at some sponsored work-related functions, approval may be given by the CEO or Managing Director for the responsible consumption of alcohol.

In these circumstances, the following restrictions apply at all work-related functions:

- Where employees choose to consume alcohol, they must do so responsibly.
- Employees must not consume excessive amounts of alcohol.
- Inebriation does not diminish an employee’s responsibility for misconduct.
- The use of illegal drugs at work related functions will not be tolerated.
- Employees must uphold an appropriate standard of behaviour at all times, consistent with the expectations set out in the Code of Conduct and Ethical Behaviour (e210007) and other workplace policies and procedures.
- Where the responsible consumption of alcohol is approved, employees must not drive any vehicle if they are over the legal blood alcohol limit and must ensure a safe means of transport from such functions.

If an employee breaches this procedure at a work-related function and acts inappropriately, the employee may be subject to disciplinary action.

8.0 OUTCOMES FOR POLICY OR PROCEDURAL BREACHES

Where an employee is found to be in breach of these procedures and/or the overarching Fitness for Work Policy (i010104) in relation to drugs and alcohol, the supervisor will refer to the relevant ELT member and Human Resources (HR) for application of the Performance Management and Disciplinary Matters procedures.

Outcomes may include:

- Being directed to undertake appropriate counselling and/or rehabilitation.
- Disciplinary action, up to and including termination of employment.
- Undergoing a follow-up test to confirm that the employee is no longer at or above prescribed limits, prior to an Authorised Doctor certifying that the employee is no longer impaired and is fit to return to their work duties.

At all times during the application of these procedures, supervisors are encouraged to seek support and advice from the relevant ELT member and HR.

9.0 EMPLOYEE ASSISTANCE PROGRAM (EAP)

Under its EAP (refer to the Employee Assistance Procedure (e230100), STEPS provides access to the services of professionally trained counsellors to assist employees in a variety of ways, including rehabilitation for drugs and alcohol abuse.

In application of these procedures, employees may be directed to attend counselling through STEPS' EAP, however, employees experiencing problems with alcohol or drugs are also urged to voluntarily seek assistance to resolve such problems to improve their wellbeing and before they become serious enough to be in breach of the Fitness for Work Policy (i010104)

Participation in itself, in a program for an alcohol/drug problem will in no way jeopardise a worker's job. In fact, successful treatment will be viewed positively. However, participation will not relieve an employee of the responsibility to comply with the Fitness for Work Policy (i010104) and these procedures.

10.0 PRIVACY AND CONFIDENTIALITY

All matters in relation to these procedures will be treated sensitively and remain strictly confidential, ensuring compliance with company requirements under the Privacy Policy (i010106).

11.0 TRAINING AND AWARENESS

STEPS will provide appropriate awareness education to employees on the effects of drugs and alcohol. The Fitness for Work Policy (i010104) will be provided to all employees at induction, and they will also be informed of this procedure.

12.0 RELATED DOCUMENTS

Document Name	Document Name
Fitness for Work Policy (i010104)	Privacy Policy (i010106)
Code of Conduct and Ethical Behaviour (e210007)	Employee Assistance Procedure (e230100)
Performance Management and Disciplinary Matters Procedure (under construction)	

13.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	9 February 2022
Effective Date	21 February 2022	**Document Number**	i051100_v3_220221

(Uncontrolled when printed)

1.4.8 Employee Assistance

1.0 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Ensure an effective relationship is established with a recognised and professional Employee Assistance Program (EAP) provider.
- Review EAP statistical information and reports that provide general information on the STEPS workforce and EAP usage, to inform relevant decision making and HR/workforce strategy.

Managers and Supervisors will:

- Create seamless access to the EAP for employees.
- Promote EAP services to employees through the application of STEPS' policies and procedures.
- Provide information on EAP within the workplace, including distributing wallet cards and brochures.
- Maintain confidentiality where EAP services are referred to employees.

Employees will:

- Utilise the EAP services at their discretion, within the scope of these procedures.

2.0 EAP PROVIDER

STEPS has secured the services of an independent provider of EAP services with Converge International to provide professional counselling services for all employees.

2.1 ACCESS TO SERVICES

The EAP provides employees, including supervisors, with access to services including external, face to face, or telephone counselling for work-related or personal issues.

The STEPS Employer Code is 86040.

2.2 ACCESS TO RESOURCES

The EAP provider releases relevant resources including informative mental health articles and tips sheets to assist in dealing with both personal and workplace issues that may impact on well-being and productivity. Resources are accessible via the Converge International Portal. To access the Converge International Portal use:

- Username: converge
- Password: eap

2.3 LEVEL OF SERVICE

The aim of the EAP is early identification and provision of short-term assistance to help resolve any work-related or personal issues that may be impacting the work performance or quality of life of STEPS' employees. Each year, employees may access up to four (4) EAP sessions.

Following short-term counselling, the EAP service provider may refer the employee to an external agency, or arrange for the employee to continue with the provider in a private capacity, at the employee's expense.

Requests for additional EAP sessions will be made through the EAP provider to the Executive Manager – Human Resources for consideration and may be approved in extenuating circumstances.

2.4 MANAGER ASSISTANCE

The EAP provider also provides supervisors with coaching and advice, and the opportunity to discuss particular people challenges and concerns. To access Manager Assist, supervisors need to contact the Executive Manager – Human Resources directly for approval.

3.0 REFERRALS

Any STEPS' employee may contact the EAP service provider for immediate support anytime (24/7) on

1300 687 327. For non-urgent consultations employees can also arrange a private and confidential appointment, at a location in close proximity to the employee via:

- Online at https://convergeinternational.com.au/contact/bookings/
- Via the Converge App available on Apple/Google Store

STEPS may use the formal referral process of the EAP provider to refer employees for counselling or psychological assessment following a specific and identifiable behaviour issue that has been adversely affecting workplace productivity or safety. Formal referrals will be managed by the Executive Manager – Human Resources.

4.0 PRIVACY AND CONFIDENTIALITY

All consultations will be conducted in complete confidence between the individual employee and the EAP counsellor and will not be communicated further unless written authorisation by the employee is given.

5.0 REPORTING

The provider will deliver statistical reports on the EAP services accessed by the STEPS workforce. All reports and information are for statistical purposes only, will be treated confidentially and are designed to protect the identity of individual employees.

6.0 RELATED DOCUMENTS

Document Name
Nil

7.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	23 February 2023
Effective Date	24 February 2023	**Document Number**	e230100_v3_230224

(Uncontrolled when printed)

1.4.9 Employee Grievance

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to promoting an environment where employees feel supported to come forward with their grievances in the knowledge that the responsible supervisor will take prompt and effective action to address grievances raised under this procedure.

1.1 DEFINITIONS

Complainant	The employee raising a grievance.
Grievance	A work related concern for which an employee wishes to obtain an action or response. It may be about an incident, situation or decision that the team member believes impacts on work performance or the work environment.
Frivolous Grievance	The nature of a grievance which has little or no weight, worth, or importance and not worthy of serious notice.
Malicious Grievance	A situation in which one employee intentionally files an untrue grievance against another employee.
Procedural Fairness	Requires those involved in the application of this policy to act fairly in their decision making processes, which may affect an individual's rights, interests or legitimate expectations.
Respondent	The employee responding to the grievance as the defending party.
Victimisation	The selective punishment or discrimination of another employee.
Vexatious Grievance	The lodgement of a grievance without sufficient grounds and serving only to cause annoyance to the respondent.

1.2 RESPONSIBILITIES

The Managing Director (MD) and/or Chief Executive Officer (CEO) will:

- Ensure that all employee grievances are resolved in an effective and timely manner in accordance with this procedure and supporting principles.

- Allocate appropriate resources (either internal or external) to investigate and resolve employee grievances.

Executive Leadership Team (ELT) and Program Manager will:

- Provide the resources to ensure that all employees are aware of this procedure and its relationship to other policies and procedures.
- Ensure that supervisors participate in regular education provided on how to deal with employee grievances and apply these procedures.

Supervisors will:

- Promptly, impartially and confidentially apply this procedure in a robust, objective manner, based on seeking resolution.
- Pro-actively engage with Human Resources (HR), who is responsible for providing independent advice and promoting an equitable process for all involved.
- Protect employees making a grievance and/or have been a witness to activities that form part of a grievance procedure.
- Identify and manage frivolous, malicious and vexatious grievances.
- Follow reasonable steps to deal effectively with grievances and minimise any risk to the health and safety of workers, clients and the wider community, whilst protecting themselves from being vicariously liable as an individual.

Employees will:

- Maintain a professional and courteous relationship with colleagues, supervisors and clients in the workplace.
- Before initiating this procedure, the complainant is encouraged to try to resolve the grievance directly with the person/s concerned. If this is not possible or appropriate, the complainant should commence the official grievance procedure.
- Report grievances appropriately and in a timely manner through this procedure.
- Maintain confidentiality and privacy in relation to all matters discussed as part of this procedure.
- When making grievances, participate seriously in attempts to resolve their grievance, not make vexatious, malicious or frivolous grievances and recognise that the person complained about, i.e. the respondent, has the right to respond to the allegations.
- When a grievance has been lodged against them, participate seriously in attempts to resolve the issues; recognise the complainant's right to raise their concerns and not victimise or harass the complainant or others involved in resolving the grievance, in any way.

1.3 GRIEVANCE PRINCIPLES

- Grievances should be handled quickly and as close as possible to their source.
- Wherever possible, grievances should be resolved by a process of discussion, cooperation and conciliation. The aim is to reach an acceptable outcome that preserves future ongoing working relationships.

- Both the employees raising the grievance (the complainant) and the person against whom the grievance is made (the respondent) will receive appropriate information, support and assistance in resolving the grievance.
- Parties may bring a support person to any stage of this procedure.
- No person (includes complainant/s, respondent/s and witnesses) should suffer any retribution if they raise a grievance or are associated with a grievance.
- STEPS recognises its duty of care and where a complainant does not wish to report a grievance, the seriousness of the grievance and the potential consequences will be considered by their supervisor. The supervisor will determine whether, should the grievance be substantiated, it is serious enough to lead to disciplinary action, and whether it involves behaviour that may harm or threaten other employees. In these cases, the complainant will be made aware of STEPS duty of care and proceed to confidentially report the matter to the relevant Program Manager/ELT or HR Manager.
- If the complainant wishes to remain anonymous, no action can be taken to resolve a grievance because procedural fairness requires that respondents be given details of the allegations made against them and have a fair chance to put forward their side. Employees can seek advice at any stage from the HR Manager.
- Employees will be encouraged to access the STEPS Employee Assistance Program (EAP) for support during any grievance procedure. Refer to Employee Assistance Procedure (e230100).

2.0 MANAGING EMPLOYEE GRIEVANCES

There are three basic steps to the employee grievance procedure:

1. **Resolution through immediate supervisor**
2. **Escalation to Program Manager/ELT member and HR Manager**
3. **Escalation to the MD and/or CEO (including possible formal external investigation)**
    - It is the expectation that most grievances can be resolved at a lower level, through advice, discussion and conciliation, at Steps 1 and Step 2.

Step 3 will only be undertaken if the first two stages could not resolve the situation satisfactorily, or if it was not appropriate to deal with the grievance at lower level (e.g. for more serious issues).

However, all grievances are different and the particular circumstances of each case will influence how it is managed. This procedure provides the steps to help promote the management of all grievances in a fair and consistent manner. At any point in following this procedure, your ELT member or HR Manager are available to assist and support supervisors and employees in seeking resolution for any grievance.

In raising any grievance, the complainant should provide the following information:

- their name, role in the organisation and the names and roles of any other parties to the grievance;
- overall nature of the grievance;
- specific details of the grievance, including:
    - when the incident or issue occurred;
    - what happened;
    - where it happened; and

  - how it happened.

- what they have done to attempt to resolve the grievance prior to raising a grievance; and
- what the complainant would like to see as the resolution

STEP 1 - RESOLUTION THROUGH IMMEDIATE SUPERVISOR

- Where the complainant has been unable to resolve the grievance themselves, they should take the matter up with their immediate supervisor. Where the grievance involves their supervisor, the complainant should refer the matter to the next most appropriate supervisor (e.g. Program Manager or ELT member).
- The supervisor will assess the grievance as presented to determine whether it is a matter that can be managed informally at this level or whether it will require a more formal process and should be escalated to Step 2. If in doubt, the supervisor or complainant can seek advice from the HR Manager and/or escalate to Step 2. Where a grievance is provided in writing, it should be treated formally and escalated to HR for written acknowledgment (Step 2).
- Where the supervisor manages the grievance informally, they should document the following:
  - information provided by the complainant;
  - the timing and details of any actions the supervisor took to resolve the grievance, including notes of any meetings with any parties to the grievance;
  - the agreed resolution to the grievance and how this was delivered to the complainant; and
  - any follow-up actions required.

Documentation should be forwarded to HR for record keeping purposes.

In any action taken, the supervisor should ensure procedural fairness for all parties involved.

Supervisors should refer to the Tips for Supervisors: Informal Grievance Management (e210101).

STEP 2 - ESCALATION TO PROGRAM MANAGER OR ELT MEMBER AND HR

- If the complainant believes the grievance has not been resolved to their satisfaction during Step 1, or the matter is in relation to their supervisor, they should refer the matter to the relevant Program Manager or ELT member and the HR Manager to be dealt with at this level.
- The relevant Program Manager/ELT member and HR Manager will discuss the matter, identify an appropriate course of action, and liaise with the MD and/or CEO who will endorse the appropriate course of action.
- The HR Manager is responsible for informing the MD and/or CEO of any grievances received at this level, and ensuring the MD and/or CEO is provided with status reports as required. In addition, the HR Manager is responsible for providing monthly reports to the Board on employee grievances.
- The HR Manager will acknowledge receipt of the grievance within two (2) business days.
- The relevant Program Manager/ELT member and HR Manager will work together to carry out the appropriate processes, which may include further informal procedures or the initiation of a formal investigation procedure.
- All grievances at this level should be resolved within three (3) weeks of receiving the grievance at this level.
- HR will maintain all records associated with the grievance.

STEP 3 - REFERRAL TO MD/CEO

- If the grievance remains unresolved, or is felt to be of such a serious nature that it cannot be resolved at Step 2, it may be referred directly to the MD and/or CEO.
- After giving due consideration to the grievance, the MD and/or CEO may do one or more of the following:
  - refer the grievance back to the relevant supervisor or to a nominee, with advice, for resolution;
  - initiate further investigation and advice;
  - seek to resolve the matter directly; or
  - if necessary, contact an appropriate outside agency.
- Any determination made by the MD and/or CEO in accordance with Step 3 of the grievance procedure will be final, save for the complainant's/respondent's right to pursue the matter outside the STEPS organisation.

3.0 OUTCOMES

- Outcomes will vary from case to case depending on the nature and circumstances of each grievance and could include:
  - the complainant gaining a better understanding of the situation and no longer feeling aggrieved;
  - the complainant receiving a verbal or written apology;
  - one or both parties agreeing, or being required, to participate in some form of counselling or mediation (internally or externally); and
  - disciplinary action, up to and including termination, as per the Performance Management and Disciplinary Matters (TBA) procedure.

4.0 FRIVOLOUS, MALICIOUS OR VEXATIOUS GRIEVANCE

- If there are grounds for believing that a grievance is frivolous, malicious or vexatious, the complainant should be informed of this and the reasons for it and told that they have a right to take the matter further as part of the procedural fairness process.
- A frivolous, malicious or vexatious grievance will be handled through the same grievance procedure.
- Complainants should be made aware at the beginning of the grievance process that if a grievance is found to be malicious or vexatious then appropriate disciplinary procedures may be invoked against them.

5.0 RECORD KEEPING

- All records in relation to the Employee Grievance Procedure (e210100) should be stored in a confidential file with HR.
- All records in relation to any disciplinary outcomes should be stored on the employees file.

6.0 EXTERNAL RESOLUTION

Employees have the right to seek external assistance at any stage in the grievance procedure and where the issue is not resolved under these procedures, employees can contact the relevant government bodies, which may include:

- Fair Work Australia
- Workplace Health and Safety Queensland
- Australian Human Rights Commission or the relevant state body

7.0 RELATED DOCUMENTS

Document Name	Document Name
Tips for Supervisors: Informal Grievance Management (e210101)	Employee Assistance Program (EAP) (e230100)
Disciplinary Action and Effective Termination (e210600)	

8.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	4 May 2023
Effective Date	12 May 2023	**Document Number**	e210100_v4_230512

(Uncontrolled when printed)

1.4.10 Employee Exit

1.0 INTRODUCTION

Whilst STEPS Group of Companies (STEPS) endeavour to sustain the employment relationship with all employees, when the employment relationship ends either at the instigation of the employee or employer, STEPS is committed to ensuring a seamless employee exit. Further, STEPS recognises the valuable opportunity presented by undertaking employee Exit Interviews to collect and analyse critical information to ensure continual organisational improvement, assist with workforce planning, develop management capability and increase employee retention.

1.1 DEFINITIONS

Industrial Instrument	Refers to the applicable Modern Award, Collective Agreement or Employment Agreement.
Resignation	The voluntary exit of a paid employee.

Termination	The involuntary exit of a paid employee.

1.2 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Demonstrate a fair, consistent and legally compliant approach to exiting employees from the organisation.
- Review and analyse employee exit information on a regular basis to improve business practices and employee retention.

Program Managers will:

- Escalate employer initiated termination processes through the appropriate delegations.
- Liaise with Human Resources (HR) to ensure these processes are followed and mitigate any risk for the organisation in exiting employees.

Supervisors will:

- Conduct employee exit activities utilising the resources developed by HR to ensure consistency and compliance.
- Complete any necessary documentation/requests from HR associated with exit activities with the exiting employee.
- Manage timeliness of employee exit procedures to ensure all exit activities are completed within the required timeframes.
- Coordinate the return of all company property from the exiting employee.

Employees will:

- Where an employee initiates the separation process, follow this procedure and complete the relevant employee exit activities and associated documentation.
- Have the opportunity to contribute to continual improvement processes by participating in an employee exit interview which will be conducted by HR.

2.0 EMPLOYEE INITIATED TERMINATION

2.1 EMPLOYEE NOTIFICATION OF RESIGNATION

Employees are required to complete and submit the Notice of Resignation Workflow Form in ConnX and attach a written resignation either in the form of a Word document or email to their Manager/Team Leader. This form should be completed in a timely manner to provide the required notice in accordance with the applicable Industrial Instrument.

HR will acknowledge the employee’s resignation via email and provide instructions for exit activities to be undertaken.

2.2 EMPLOYEE EXIT INTERVIEWS

HR will contact each exiting employee who has resigned and provide the opportunity to undertake an Employee Exit Interview.

Access to feedback provided during an Exit Interview will be restricted to HR, the Managing Director and Chief Executive Officer. The Executive Manager – HR at its discretion may share feedback from an Exit Interview with appropriate management representative/s.

Feedback provided during an exit interview will be collected and stored on a secure online platform.

Where employee exit information identifies a specific high risk, the Executive Manager – HR will discuss the individual exit information with the Managing Director and/or Chief Executive Officer to identify risk elimination or mitigation actions to be undertaken.

3.0 RELATED DOCUMENTS

Document Name
Nil

4.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	2 November 2023
Effective Date	8 November 2023	**Document Number**	e210300_v4_231108

(Uncontrolled when printed)

1.4.11 Employment References

1.0 INTRODUCTION

Exchange of information between employers maximises the opportunity to evaluate an applicant's past job performance to be fitted into the positions for which they are best suited. Where possible, STEPS Group of Companies (STEPS) wishes to provide and receive accurate information on the individuals with whom it deals. However, some precautions are necessary to safeguard the organisation against litigation.

1.1 DEFINITIONS

Referees	General Manager, Business Manager or above.
References	Refers to material obtained or provided, in confidence or otherwise, to prospective employers to be used to assess a candidate's suitability for a position.

The purpose of references is to obtain information from a third party, providing a factual check on an applicant's employment history, qualifications, experience and/or an assessment of the applicant's suitability for the position in question. Checking references involves contacting previous employers, supervisors, schools, and other relevant parties to verify key employment and educational information and learn more about an applicant's background, experiences, and skills.

Reference checks can help to verify the claims made by applicants in their interview and assist hiring managers to make more informed hiring decisions.

Seeking employment references is a separate matter from requiring police record checks, Right to Work or licencing checks, and this procedure does not apply to police record checks, Right to Work or certification checks.

1.2 PURPOSE

This procedure seeks to ensure that the information needs of STEPS, the applicants, and the other organisations concerned are met in a manner that places no party at risk of misunderstanding or conflict.

Intentionally providing inaccurate information about an individual or withholding critical information about an employee or former employee could result in a claim for misrepresentation from the new employer or defamation from the employee with the potential to seek compensation for damages.

1.3 RESPONSIBILITIES

Human Resources (HR) will:

- Review and approve requests for reference checks prior to being provided to external parties.
- File reference documents in the employees file utilising the Human Resources Information System ConnX.

Referees will:

- Only provide written reference checks for roles and employees that directly report to them.
- Only provide reference checks approved by Human Resources (HR), to ensure organisational consistency and minimise any risk of exposure for the organisation in making reference statements under this procedure.
- Meet the requirements for record keeping, ensuring that only written references are provided.
- Participate in education and training to understand their duty of care under common law to the former employee that the information in the reference provided is correct and fair.
- Employers have an additional duty of care to the prospective new employer to truthfully portray the employee’s or former employee's professional attributes.

2.0 PROVIDING REFERENCES

STEPS will, in most cases, provide references for employees and former employees where the employee or former employee has contacted the referee and requested to do so. However, there is no obligation on the organisation to do so.

References will be provided only to appropriate parties. Before providing a reference, the referee should verify the identity of the person requesting the reference. If in doubt about the identity of the person requesting the reference, the referee shall NOT provide a reference. The referee should not give out any information to parties who do not have a legitimate “need to know”.

References must only be provided in writing and subject to approval by HR. Written references shall be clearly marked ‘Private and Confidential’ and, once approved, must only be disclosed to the appropriate parties.

In considering whether to give a reference, and in determining the content of any such reference, referees must not discriminate on any grounds covered in STEPS Anti-Discrimination and Equal Opportunity Policy, STEPS Recruitment and Selection Policy, STEPS Privacy Policy or that breaches the Privacy Act 1988.

When providing references, referees shall

- Take reasonable care
- Provide only information as outlined in the reference template

- Provide information which is as far as possible true, accurate and fair, and which does not give a misleading impression
- Not make any publications or statements about an individual which are defamatory or could bring STEPS into disrepute
- Ensure they comply with any policies and procedures of STEPS concerning confidential information and privacy
- Not extend into information of a personal nature
- Limit the information given to the employee's or former employee's job-related performance.

A staff member can act as a personal referee for any individual. However, such references must NOT be provided via the staff member's STEPS email and must say that the reference is being made in a personal capacity. On NO account should a personal reference be identified on STEPS letterhead or any form of company communication or in any way suggest that STEPS endorses the reference.

3.0 ACQUIRING REFERENCES

Acquiring references is normally undertaken through STEPS Staffing Solutions. In the rare event outside of this, please follow these guidelines.

References should only be obtained directly from the referee provided by the person requesting the reference.

Before requesting a reference, the staff member should verify the identity of the person providing the reference. If in doubt about the identity of the person providing the reference, the staff member should ask for the request in writing.

Reference information requested shall be in line with the reference template.

When these references have been made, the references shall only be used for the purpose of evaluating the applicant against the position applied for.

The Recruiter or Hiring Manager may, at its discretion, seek written references and/or telephone references.

Where telephone references are sought, the person seeking the reference should:

- Ensure they are speaking to the appropriate person in the organisation
- Make it clear to the referee that they are making notes, that a copy of the notes may be provided to the person if they request it, and that the referee's name will also be disclosed
- Be sensitive that legal considerations may limit the amount of data/information a referee is prepared to give
- Make clear notes of their conversation and secure these on the applicants file at the earliest opportunity with the other material relating to the recruitment.

4.0 CONSENT

Current and former employees seeking a reference, should advise HR of their intention and seek approval. Where no contact has been made, consent will not be implied and no reference will be provided. If the person seeking a reference has made attempts to contact HR for approval, and HR has not responded (for any reason), consent will not be implied, however the referee must use their best endeavours to contact HR and ascertain approval (to be granted or withheld at STEPS' sole discretion). At no time will HR's silence to a request for a reference be deemed consent, and a reference must not be provided without HR, or higher management, approval.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Anti-Discrimination and Equal Employment Opportunity Policy (i010102)	Privacy Policy (i010106)
Recruitment and Selection Procedure (e200201)	Reference Check (e340501)

6.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	24 June 2024
Effective Date	5 July 2024	**Document Number**	e340500_v1_240705

(Uncontrolled when printed)

1.4.12 Flexible Working Arrangements

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) recognises that flexibility is becoming increasingly important for attracting and retaining diverse talent in the workplace. Flexible working can drive employee engagement and productivity as well as boosting employee well-being and happiness.

Flexible working arrangements should not be confused with minor and ordinary work adjustments such as taking time off as personal/carer's leave, compassionate leave or parental leave.

1.1 DEFINITIONS

Flexible work	A flexible work arrangement is an agreement between a workplace and an employee to change the standard working arrangement to better accommodate an employee's commitments out of work. Flexible working arrangements usually encompass changes to the hours, pattern and location of work.
Working from home	A home-based, safe workspace in an environment that supports the accomplishment of work.

2.0 WHO CAN REQUEST FLEXIBLE WORK?

The Act allows for employees (other than a casual employee) who have worked with STEPS for at least 12 months can request flexible working arrangements if they:

- are the parent, or have responsibility for the care, of a child who is school aged or younger
- are a carer (under the Carer Recognition Act 2010)

- have a disability
- are 55 or older
- provide care or support a member of the household or immediate family who requires care and support because of family or domestic violence
- a member of their immediate family or household, are experiencing family and domestic violence.
- employees who are pregnant

Casual employees can make a request if:

- they've been working for STEPS regularly and systematically for at least 12 months
- there's a reasonable expectation of continuing work with STEPS on a regular and systematic basis.

STEPS recognises the benefits of a diverse workforce across all ages and genders and supports the well-being of its workforce. For this reason STEPS will consider flexible working requests from employees who fall outside the requirements as stated above.

2.1 WHAT CHANGES CAN BE REQUESTED

Flexible work arrangements can cover:

- hours of work (e.g. changes to start and finish times)
- patterns of work (e.g. split shifts or job sharing, compressed working week)
- locations of work (e.g. working from home).

A flexible working arrangement may involve a change in working arrangements for a fixed period or on an ongoing basis to accommodate a range of personal commitments.

3.0 HOW TO SUBMIT A REQUEST

3.1 FORMAL REQUESTS

If it is a short-term arrangement for a few weeks or a couple of months, designed to meet a specific employee need, then an informal arrangement should be sufficient in most instances.

This informal arrangement between an employee and line manager/supervisor must be documented in emails where the employee states the requested change (including change requested, the reasons for the request and the duration) which would then be approved by the line manager/supervisor.

If it is a long-term prospect (longer than two months), then a formal arrangement may be more beneficial to everyone.

3.2 FORMAL REQUESTS

Where the request for flexible work arrangements is long-term, the request must be emailed to the HR Team at hr@stepsgroup.com.au explaining:

- what changes are being asked for
- the reasons for requesting the change
- the impact on work, and how any negative impact could be mitigated
- perceived benefits.

Consider a trial period as this will give both you and your line manager/supervisor an opportunity to see how it can work and it gives everyone a chance to decide if a different type of flexibility might better suit the needs of the employee and the business, or not. A trial of around three months is usually sufficient and during this time the flexible working arrangement should be actively monitored.

4.0 CONSIDERING THE REQUEST

HR will consult with the Line Managers/Supervisors to discuss and document the following:

- the needs of the employee
- consequences for the employee if changes in working arrangements aren't made
- any additional costs that will be incurred if the Flexible Working Arrangement is put in place
- impact on the team
- ability to measure productivity
- any negative impact on customer service
- any reasonable business grounds for refusing the employee's request
- the Home Safety Self-Assessment Checklist (e250101) needs to be completed and returned to identify any risks.

The HR Team will then:

- present the information to the CEO or MD for a decision (if further consultation is required, this will be coordinated by HR)
- advise the Line Manager/Supervisor of the decision
- prepare and email the written response, signed by the CEO or MD, to the applicant cc'ing the Line Manager/Supervisor
- save the documentation in the employee's file.

A written response **must be provided within 21 days** advising if the request is approved or refused. Twenty-one days commences from the date the request is received in writing by the Line Manager/Supervisor.

If a request cannot be approved due to reasonable business grounds, the manager/supervisor must undertake consultation with the employee to reach an agreement. If no agreement can be reached, the response must contain the reasons for the refusal.

4.1 REASONABLE BUSINESS GROUNDS

The following could be reasonable business grounds:

- the requested arrangements are too costly
- other employees' working arrangements can't be changed to accommodate the request of the individual employee
- it is impractical to change other employees' working arrangements or hire new employees to accommodate the request
- the request would result in a significant loss of productivity or have a significant negative impact on customer service.

5.0 EXPECTATIONS AND RESPONSIBILITIES

5.1 LINE MANAGERS/SUPERVISORS

When a line manager/supervisor has a team where flexible working arrangements are in place, it is imperative that they do the following:

- Establish good communication to keep all team members up to date using collaborative software, video conferencing or phone calls.
- Ensure all team members (including those working flexibly) attend regular meetings over video conferencing or schedule meetings when all team members are in the office and can attend are face to face.
- Sensitive or complex discussions need to be had ad hoc via face-to-face meetings or video conferencing. Email is a less effective and less successful way for discussing sensitive or complex topics.
- Out of office notifications are handled by an automatic email response and phones are diverted to the employee's work mobile or to another team member.
- Set very clear goals/outcomes or objectives for the team including those working flexibly. These goals, outcomes or objectives must have quality, time and results clearly communicated and understood as this will ensure accountability.
- Allow employees to work autonomously on how outcomes are achieved.
- Provide clear, factual feedback on how employees are tracking in relation to their performance objectives.
- Ensure ICT is notified of the arrangement to ensure information security protocols are followed.
- Ensure the employee is aware of their responsibilities under the Mobile Device Policy (6002100) which refers to the protection of mobile computing equipment by:
    - prevention of unauthorised access by persons living or working on the location where the teleworking activity is performed
    - appropriate configuration of the local network used for connecting to the Internet (i.e.WiFi password)
    - protection of the organisation's intellectual property rights, either for software or other materials that may be protected by intellectual property rights
    - process for return of data and equipment in the case of termination of employment
    - minimum level of configuration of the facility where teleworking activities will be performed
    - permitted and forbidden types of activities.

5.2 EMPLOYEE WORKING FLEXIBLY

When considering or commencing flexible working arrangements, an employee must be prepared to do the following:

- Use communications technology such as videoconferencing and collaborative work platforms. Be available during your scheduled work hours for ad hoc communications.
- Ensure all ICT policies and procedures relating to access, use, storage, and destruction of data are adhered to at all times.
- Find ways to make the results you deliver transparent to your line manager / supervisor and team. Ensure you have clear understanding of your performance expectations, if unclear ask for further guidance or information.

- Use appropriate channels to communicate your hours, location, or other availability. Some people use their signature block to provide a clear and accessible reminder e.g. Monday–Thursday 8 am to 4 pm
- Plan your work and allocate sufficient time and resources to achieve it. Make sure that you are able to work without too frequent interruptions. Draw clear boundaries. You need to draw boundaries with both your colleagues and your family and friends to ensure that your work time is clearly defined from your non-work time to show clearly that you're unavailable during work.
- Any equipment or ICT assets provided to the employee by STEPS will only be used by the employee (no family members) for work purposes and will remain the property of STEPS.
- STEPS is committed to providing a safe work environment which includes home based offices. For this reason, all safety and wellbeing requirements that apply in your usual work location also apply when you are working from a Home-Based Office (HBO).
- Work Health and Safety requirements are stated in the Home Safety Self-Assessment Checklist (e250101) which will be completed by the employee with any resulting actions noted. This will need to be reviewed every 12 months at a minimum.
- Maintain open and honest communication with your line manager/supervisor, especially if you are experiencing difficulties or if the arrangement is not working as expected.

6.0 REVIEW OF THE WRITTEN FLEXIBLE WORK ARRANGEMENT

Working flexibly may work well from the start of the arrangement, where a productive working relationship is maintained with your line manager/supervisor and your team. However, we may need to make some adjustments to achieve a more effective arrangement.

For this reason, it is recommended that flexible working arrangements are reviewed annually during a performance review at a minimum.

If it becomes necessary, for operational reasons, to remove an agreed flexible work arrangement STEPS will clearly communicate the reasons for the change and provide adequate notice to enable the employee to make any necessary arrangements.

7.0 BREACHES OF FLEXIBLE WORKING ARRANGEMENTS AGREEMENT

If an employee breaches any of the conditions forming part of the flexible working arrangements this may result in disciplinary action up to and including termination.

If an employee believes their line manager/supervisor is breaching the Working from Home Agreement (e250102), they are encouraged to raise the concerns directly with their line manager/supervisor; however, if this is unsuccessful or cannot occur the employee should raise their concerns with the Executive Manager – HR.

8.0 RELATED DOCUMENTS

Document Name	Document Name
Home Safety Self-Assessment Checklist (e250101)	Mobile Device Policy (6002100)

Working from Home Agreement (e250102)	Working from Home Work Health & Safety Guide (e250103)

9.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	13 July 2023
Effective Date	14 July 2023	**Document Number**	e250100_v5_230714

(Uncontrolled when printed)

1.4.13 Guidelines for Staff Supervision

1.0 INTRODUCTION

STEPS recognises that our staff working in the disability sector strive to do the right thing for the people they support. Staff may however look to supervisors and managers for guidance and advice on how to appropriately uphold clear safe boundaries while meeting client needs. Managers and supervisors may also need to monitor and mitigate factors of staffing practices which create risks and potential for harm to occur to people with disability or to themselves.

This procedure serves to support supervisors, team leaders and managers in providing a prevention-focussed approach to managing the risk of harm to our clients with disability and to staff by identifying risks associated with staffing practice, and offers supervision and management approaches to address them.

Staff can expect that their supervisor will reach out and connect with them on a minimum of six-monthly basis to ensure they are feeling supported, have access to resources that require a high quality of service delivery and to discuss any professional development opportunities. It is important that staff take an active role in this meeting, by being prepared and transparent.

1.1 DEFINITIONS

Supervisor	The term ‘supervisor’ is used generically in this document to refer to line managers, coordinators, team leaders, managers and others with responsibility for supervision of staff who support people with disability.

2.0 THE RIGHT KIND OF SUPERVISION

The relationship between frontline staff and their supervisors – including line managers and team leaders – is critical to ensuring quality and safe services are provided to people with disability. To support positive supervisory relationships, supervisors should ensure that:

a) They are skilled in the requirements of their role and have appropriate time to do it, including:

- understanding of STEPS' values, expectations, policy and practice regarding safeguards for clients
- creating opportunity for regular contact – remote or in person - with staff they supervise
- maintaining knowledge of what is actually happening on the ground for people accessing services
- being available and providing ongoing support and mentoring to support staff
- monitoring whether staff are meeting expectations and take responsibility for addressing underperformance (or seeking support to address underperformance where necessary).
- Ensuring they have the ability to balance a diverse range of workload demands including administrative tasks, providing direct supervision, managing workflows, handling or overseeing feedback and complaints, etc.

b) They act as positive role models, by:

- demonstrating positive practice leadership in their actions and approaches
- setting expectations about service cultures and reinforcing as required
- ensuring staff are trained in STEPS' values, codes of conduct and the rights of people with disability
- training staff to understand safeguarding-related policies and procedures, including complex issues like managing the safety of the person whilst upholding their right to take risks
- reinforcing the importance of listening to people with disability, finding ways to assist people's decision-making processes and responding to requests with diligence, courtesy and speed

c) They acknowledge and encourage good practice, by:

- encouraging reflective practice
- placing workers who demonstrate good practice in positions of responsibility to act as role models, including mentoring/buddy roles with new workers, team champions for specific issues or practice areas
- building a sense of purpose where each team member, sees how they are contributing to a bigger picture of change for people with disability and the broader community

d) They recognise and challenge poor practice

Poor practice can be an early indicator of other unseen problems. Supervisors need to recognise that poor practice may coincide with boundary blurring which precedes boundary crossing; for this reason, if left unchecked poor practice may increase to risk of harm. Monitoring and addressing poor practice also demonstrates the supervisors' commitment to safeguarding against risks of harm. Supervisors should:

- be skilled, and regularly re-skilled, in identifying signals of unacceptable practice and behaviour
- have the skills and confidence to address identified unacceptable behaviours and a clear understanding of the scope of their responsibility to address them
- encourage and support staff to consider and improve their practice, for example, assisting staff to identify ways in which they may be limiting choice for people with disability
- monitoring incidents and noting any trends where staff are involved

- be confident that they have the full support of their own managers and senior leaders within their organisation when tackling issues related to poor practice, including access to Human Resources support and advice

e) They use staff appraisals and probationary periods effectively, by

- being clear with new staff on the purpose of probation to review and assess suitability for a position and with the organisation
- assessing and monitoring staff performance, capabilities and conduct against tangible, agreed KPIs and responding early to any concerns
- documenting or noting any direction given to staff in relation to their performance, practices and/or conduct
- making full use of the probationary period to ensure a clear understanding of the expectations and requirements of the role and to identify areas where the employee may need further training and support
- understanding that different roles require different levels of supervision at different times (e.g. supervision may be higher at the start then ease off as skills are acquired, or may increase while concerns are worked through)
- recognising new staff provide ’fresh eyes’ and are an important source of information about staff behaviour or performance and where there are issues with the culture of the organisation

  (Refer for Performance Review Procedure (e220200)

f) They facilitate active feedback cultures by:

- Seeking feedback from their staff, people with disability, families, carers and other stakeholders about what is working, what’s not working and the way that things are done
- Using a range of feedback mechanisms, including one-on-one discussions; team and/or house meetings; informal chats; service user feedback groups; suggestion boxes. More formal approaches, such as independent facilitator or evaluators, can also be useful.
- Avoiding authoritarian styles so people feel comfortable about raising issues
- Responding promptly, appropriately and fairly to any issues and complaints raised so that people hear about and understand the positive outcomes of a complaint having been made
- Using supervision and/or informal chats with staff to address any identifiable issues and concerns directly
- Reminding everyone “there is nothing so big or so small that we cannot talk about it” and “it’s OK to ask, it’s OK to get things wrong, but not OK to cover things up”
- Reporting complaints to their own manager promptly and acting to resolve the factors contributing to the complaint showing a commitment to continuous improvement processes
- Reinforcing to staff the importance of cooperation with independent evaluators such as Official Community Visitors (or jurisdictional equivalent) and the positive impact their involvement can have on client wellbeing

3.0 STAFF TRAINING AND COMPETENCE

STEPS recognises that staff in the disability sector come from many different backgrounds and professional experiences. Some have no lived experience of disability or may not have worked with people with disability before. STEPS acknowledges that we have a duty of care to ensure all staff have the right skills to do their job, and are aware that their performance impacts on the safety and wellbeing of people with disability they support. Things for managers and supervisors to consider when rostering, managing, inducting, training and developing workers include:

a) Understand preferences of people with disability and match staff accordingly. Try to accommodate people's preference for a certain type of staff member – for example, women who request female-only staff, or people who request a staff member who can assist with a specific cultural practice. Recognise that this requires managing and balancing legitimate preferences of service users, rosters and employee feelings.

b) Ensure skills match the job or task undertaken. Staff need to have the right skills for the job they will be doing. Check applicant skills and experience during the recruitment process and monitor during induction. For example, if people are undertaking personal care then they should have the right level of experience, empathy, training and supervision. Staff also need the right combination of hard and soft skills. Hard skills might include qualifications and experience in providing specific medical supports. Soft skills include attitudes, values, aptitudes and flexibility to do their job.

c) Provide a quality induction which is clear, accessible and comprehensive for all staff. This should include STEPS' values, rights of people with disability and examples of good and poor practice, as well as skill-specific training tailored to each role or worker. In some circumstances, this may mean not allowing staff to commence particular types of service delivery until they have undertaken particular modules of induction and training.

d) Limit roles for new or inexperienced staff until they are skilled and familiar with the individual needs of the people with disability they support and the specific processes involved in providing support. Pair with experienced and trusted staff where possible.

e) Maintain ongoing training. Induction should be the starting point for a range of ongoing training and professional development activities. These are also a critical part of ensuring staff remain engaged in their work. Staff should be offered targeted safeguarding training including:
   - understanding and supporting human rights of people with disability
   - person-centred, active support
   - understanding abuse, its causes and signals of abuse
   - reporting processes and procedures
   - supporting people with behaviours of concern without use of restrictive practices
   - supporting people with complex communication needs
   - local privacy legislation and requirements
   - reflective practice in the context of human rights

Targeted training can be used to encourage staff to take a consistent approach to the management and handling of issues, complaints and risks. This is the preferred approach, rather than improvising responses which have the potential to generate even greater risks (for example, in extreme cases, poor training can lead to increased risk of unauthorised restrictive practices or unchecked abusive behaviour against clients).

4.0 STAFF DEPLOYMENT AND SUPPORT

All staff should be supported to work in a safe way that mitigates risks for them and the people they support. This means supervisors should be aware of:

a) Staff morale, job satisfaction and working conditions

- Create opportunities for staff to give feedback and for you to give feedback to staff
- Acknowledge and praise good practice – especially in difficult work situations
- Identify and acknowledge challenges staff may face and provide them with appropriate responses and support

- Staff may need support to manage stress, anger and frustration, regardless of the cause
- Take seriously and respond to legitimate support worker concerns
- Use Work Health and Safety strategies including those identified in NDS's Disability Safe website and resources.
- Provide appropriate critical incident debriefing as soon as possible when required.

b) Increased absenteeism

Where staff culture issues are not well managed, it can contribute to high rates of unplanned leave and staff turnover. Supervisors should be aware of how this can compound the original issues and create additional risk for people with disability. Understaffing can compound issues through:

- limiting the staff available to support people with disability safely
- increasing reliance on new and inexperienced staff
- increased exposure of people with disability to unfamiliar or incompatible staff
- placing expectation on available staff to work additional hours, which increases the risk of staff burnout, accidents and injuries
- less time and flexibility around routines, increasing risk of development of a more rigid or controlling culture
- potentially filling vacancies with people that might not normally have been employed under other circumstances – creating a risk of lower quality standards

c) Reliance on casual agency staff

Supervisors may need to use casual agency staff to meet the needs and preferences of the people they support. Whilst this can require a quick turnaround time, in these circumstances, supervisors should take steps to plan ahead to minimise risk of harm to people with disability. Suggestions include:

- **Forming relationships with STEPS Staffing Solutions and other recruitment agencies** – meet with STEPS Staffing Solutions to understand their approaches and procedures. Discuss approaches to recruitment, pre-employment screening and background checks, qualifications and induction processes and if they meet your own standards. Only use agencies – and staff - you are satisfied can meet your standards and those of the people they will support.
- **Being clear about your expectations** –ensure that the labour hire firm is clear on the type of worker required and what they will be expected to do. This will allow them to match your requirements from within their staffing pool and identify the most appropriate person to send.
- **Being clear about expectations of people with disability** – work with the people using your service to identify their staffing preferences and include these in the brief.
- **Providing feedback** – build feedback processes into your ongoing relationship with the labour hire agency. Include any feedback from people with disability. Use this to develop a known 'pool' of preferred and trusted staff.
- **Taking into account the need for special induction or specialist training** required beyond that provided by the agency, including WHS and reporting
- **Providing access to internal staff** prior to beginning of their shift. Where this is not possible, use remote support options
- **Considering the need for supervision** and open communication by/with casual agency staff
- **Providing clarity for staff** on why casual agency staff might be required and setting expectations on working together
- **Implementing methods for seeking feedback** from agency staff to gain outsider perspectives

- Considering that people with disability may become anxious about staffing changes or receiving supports from unfamiliar people, and using matching of agency staff to service user preferences where possible.

5.0 STAFF ATTITUDES, BEHAVIOUR AND VALUES

The disability workforce is richly diverse, with staff bringing a range of personal and cultural values to their roles. Whatever their personal values, staff should be aware that they have a responsibility to the people they are supporting and to the values of your organisation when at work. Some staff may need guidance and advice about what attitudes, behaviours and values are appropriate when supporting people with disability. Supervisors should be aware of some of the potential risk indicators:

a) Attitudes toward people with disability

- The way staff talk about people with disability is an indicator of how they perceive their job role. This includes comments in the workplace, in public away from work, on social media and in private conversations.
- Be clear in your code of conduct that any negative, patronising, degrading or insulting comments about people with a disability will, where proven, result in disciplinary action which may include termination of contracts.
- Be aware of staff not treating people with disability as equals, or viewing people as having fewer rights, lower social status or being ’less than human’ (‘othering’). Such attitudes can be reinforced by generational or cultural factors, for example where people have less understanding of disability rights, and may be used to justify staff actions including poor levels of service, punishments or other forms of abuse, neglect and exploitation.
- Infantilising (treating adults with disability like babies and/or children) should be challenged. Infants are seen as having fewer rights. Treating adults like children can also deny access to relationship and sex education which are important safeguards for people with disability.
- Challenge low expectations. Staff should have the highest expectations for the people they support and support them to achieve their goals and ambitions to the fullest extent possible.

b) Personal values

- Supervisors should be mindful of staff attitudes and behaviours that might reflect on their suitability to support people with disability. These include:
  - Bullying, aggressive or forceful behaviours towards others
  - Sexist, racist, culturally insensitive or homophobic comments, attitudes or actions
  - Inappropriate expressions of beliefs, attitudes and values toward the people they are supporting – for example, where staff religious values may be at odds with a person’s sexuality
- Staff should also understand how teasing and joking can be perceived differently by people and can contribute to cultures where picking on people is seen as acceptable.

6.0 MONITORING PROFESSIONAL BOUNDARY VIOLATIONS

The personal, often intimate nature of disability support work creates some unique relationship challenges for people with disability and staff. Embedding person-centred approaches based on positive relationships between staff and the people they support is a critical safeguard. It can also lead to genuine, meaningful connections between people with disability, paid staff and volunteers. However, there may be rare occasions when predatory or opportunistic people take advantage of this trust and exploit these relationships.

In addition to ensuring all staff under their supervision are adhering to the guidelines in the Professional Boundaries Procedure (3041200), Supervisors should also monitor risk of exploitations and development of special relationships as per below.

Risk of Exploitation

- Supervisors should monitor and raise awareness of staff actions that can lead to exploitation of people with disability. Examples include:
  - asking people with disability to pay for staff drinks or meals
  - borrowing and lending of money, clothing or possessions
  - use of a person's support time to undertake personal tasks or take phone calls
  - encouraging a person to commit crimes
- As individualised funding becomes more commonplace, people with disability will have more choice and control. However this may increase risk of financial exploitation for some people with disability.

Development of 'special relationships'

Supervisors should:

- be aware of any overly close or intimate relationships between staff and people they support. Examples include where a staff member always wants to work with the same person to the exclusion of others, or who finds reasons to take someone to their private home.
- be mindful of uneven power dynamics in relationships between staff and people they support. This might include a dominant or charismatic staff member who overly influences or leads people, or staff who deliberately seek relationships with people with disability as a way to address their own needs.
- ensure people are supported by a number of staff and not rely on one individual
- discourage exchanging of gifts and provide clear guidance on expectations governing the receipt of gifts by staff members. Be aware of any overly generous, inappropriate or incongruous exchanging of gifts
- remind staff who spend time with a person they support outside of their work time that they are still subject to the organisation's policies and procedures. This includes participation in birthdays and other special events where staff are not rostered to work
- provide training and support in maintaining professional boundaries and negotiating sensitivities of closer working relationships.

7.0 RELATED DOCUMENTS

The above information is provided as examples of general good practice. It should be considered in context of local relevant legislation and policy settings, including:

Document Name	Document Name
Performance Review Procedure (e220200)	Professional Boundaries Procedure (3041200)

8.0 GOVERNANCE

Document Owner	Chief Executive Officer	**Approval Date**	14 July 2022
Effective Date	19 July 2022	**Document Number**	e240001_v2_220719

(Uncontrolled when printed)

1.4.14 Induction

1.0 PURPOSE

STEPS Group of Companies (STEPS) has a formal process to induct all new workers. The purpose of the induction process is to ensure new workers (i.e. employees, labour hire, student/work experience placement) are provided with important information about STEPS including the expectations for performing their role, to assist them to contribute to the STEPS team in a timely manner, whilst meeting legislative requirements.

2.0 RESPONSIBILITIES

Executive Leadership Team will:

- Demonstrate an integrated approach to inducting workers into the organisation.
- Allocate the financial and other required resources to deliver Induction activities.
- Work with Human Resources, who will develop, maintain and review induction activities.

Managers and Supervisors will:

- Ensure compliance with mandatory induction training requirements.
- Ensure that all on-boarding requirements have been completed prior to the worker commencing and that their work area is ready on their first day.
- Conduct induction activities utilising the resources developed by Human Resources and locally on-site to ensure consistency and compliance.
- Evaluate the induction learning of new workers to ensure the learning is embedded in their on-the-job activities.
- Complete the documentation associated with the induction activities with the new employee and upload to the licences section of the Human Resource Information System, ConnX, within the required timeframes.

Workers will:

- Participate in the induction process.
- Complete the documentation associated with induction activities.
- Participate in induction activities that have a direct relationship with the capability requirements for their role.

3.0 STEPS INDUCTION

Workers will complete their induction in a timely manner on commencement. Where a worker changes their role or the way they are engaged with STEPS, they may be required to complete all or specific components of the induction, as relevant to the change in role or engagement.

The STEPS induction includes the following key components to be completed by the relevant workers, in the timeframes, as outlined in the table below:

Induction Component	When to be completed(from commencement date)	Who to complete
Corporate Induction	Within 1 day	Relevant workers
Site Orientation including WHS compliance	Within 2 days	Relevant workers
Online Corporate Induction (incorporating WHS)	Within 1 week	Relevant workers
Completion of Induction Checklist - Employee (i070101)	Within 2 weeks	Relevant workers
Departmental/Stream Specific Induction	As established by Department	Relevant workers
NDIS Worker Orientation Module & NDIS Code of Conduct (e350022)	Within 1 day	Relevant workers

3.1 RECORD KEEPING

- Workers will complete all required documentation throughout the induction process.
- Employees are responsible for uploading qualifications and licences relevant to their role in ConnX.
- Supervisors will ensure that all completed documentation associated with induction activities is uploaded to the HRIS, ConnX, within the required timeframes. For labour hire, student/work experience placements, email completed documentation to HR for filing electronically.

3.2 REVIEW OF INDUCTION

Induction resources and content will be reviewed when there are changes to organisational policy or procedures, legislation or regulatory requirements that impact on the induction process, and at least every two years, to ensure relevance and compliance.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Deed of Confidentiality and Restraint (i070107)	Induction Checklist - Employee (i070101)
NDIS Code of Conduct (e350022)	

5.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	18 December 2023
Effective Date	30 January 2024	**Document Number**	i070100_v4_240130

(Uncontrolled when printed)

1.4.15 Leadership and Management of Sites

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is a diversified company servicing across Australia with physical locations in Queensland, Tasmania, and the Northern Territory.

It is likely that STEPS sites will have staff who are responsible for providing different services, under different programs/contracts, to different customers.

To be able to provide day to day supervision of a site and give staff access to appropriate management expertise and support to achieve outcomes, STEPS has implemented a matrix / hierarchical organisational structure. This means that staff have a site manager generally called a Business Manager or Operational Manager. For the purpose of this document, we will call this role the Geographic Manager. In addition to this role STEPS has Program Executive Managers not located at site (with required subject matter expertise).

A Program Manager has primary responsibility to deliver on contract outcomes, while the Geographic Manager has overall site responsibility. Staff line management will differ across sites but will be clear in individual role descriptions. Geographic managers may not have direct line management of some staff at site however they are accountable for day-to-day supervision of staff at site, positive workplace culture, and to understand the unique diversification of their local communities.

Facilitating this matrix structure makes it possible for STEPS to meet local community needs and maximise resources for efficiencies.

1.1 DEFINITIONS

Diversified Company	Is a company that has multiple, unrelated businesses.
Unrelated Businesses	Are businesses which: • Require unique management expertise • Have different end customers • Provide different services or produce different products
Matrix Organisational Structure	A matrix organisational structure is a company structure in which the reporting relationships are set up as a grid, or matrix, rather than in the traditional hierarchy which means employees have dual reporting relationships - generally to both a program manager and a geographic manager.

Hierarchical Structure	Refers to a vertical chain of command where decisions are made at Executive level and feed down to all employees
Functional Support Teams	This is a variant of the functional structure, with the top executives based in a home country, with the reporting segments being comprised of regional managers. This insures that demands in different markets are being met in a localised fashion.

2.0 RESPONSIBILITIES

As there are a number of people contributing to the success of the site, programs, and services delivered, it is important that all parties are actively involved in the delivery and of their individual responsibilities and accountabilities.

2.1 PROGRAM MANAGER

The Program Manager is responsible for:

- Program and individual performance against Key Performance Indicators (KPIs)
- Induction into the program or contract
- Coaching and professional development
- Program or contract advice and guidance
- Program or contract performance monitoring and reporting
- Communication across geographic locations to staff performing the same services

2.2 GEOGRAPHIC MANAGER

In most cases a Geographic Manager will hold the role of Business Manager or Operational Manager.

Both Business Managers and Operational Managers are responsible for:

- Building a site culture that supports the organisation’s values and Code of Conduct and Ethical Behaviour (e210007)
- Monitoring attendance and punctuality of all site employees
- Site orientation (including general evacuation and first response)
- Organisational Induction
- Work Health and Safety
- Approve expenses for the program as indicated in accordance with the Delegations Register (i010601)

In addition to the above, Business Managers are also responsible for:

- Effectiveness of the team within the site.
- Local management of client/student related concerns in collaboration with Program Manager
- Resource allocation within the site
- Organisational Communication
- Human Resource matters at site (conflicts) management including, but not limited to recruitment and selection, performance management and grievances. Human Resource function will support where required.

- Whilst acknowledging program employees at a site will be reporting to their Program Manager it is expected the Geographic Manager will keep up to date with the performance of program employees, any significant issues facing programs or the employee and be able to support excellent performance at their site.

2.3 EMPLOYEES

- Understand expected performance outcomes and deliverables.
- Understand the roles of Geographic Manager and Program Manager reporting procedures to line manager and contract manager
- Take the initiative to suggest improvements to processes within the site, or organisation to meet the needs of your customers
- Work with your managers to establish how each manager will capture information and have input into your performance evaluation
- Maintain a regular dialogue with the Program Manager to keep him/her appraised of your performance against established KPIs and role responsibilities
- Maintain communication with the Geographic Manager to:
  - assist in the allocation of resources and
  - build an understanding of your role’s expectations, challenges, and successes
- Identify conflicting priorities and broker discussions between managers to clarify any confusion
- In circumstances where the Program Manager is not able to provide the information or advice required to deliver the program escalate the issue to the next level of management
- Share your knowledge and skills with other staff from other disciplines as this strengthens the overall site team
- All staff are responsible for maintaining the culture of the site and keeping colleagues accountable to the expectations.

3.0 COMMUNICATION

An inclusion approach to communicating the following to all staff:

- Achieve our strategic direction and business goals
- Maintain a coherent organisational culture
- Promote innovation
- Understand local needs
- Deliver successful performance
- Provide a supportive work environment for all employees within a variety of programs, and
- Co-ordinate activities across functions and programs

If a circumstance arises in which the Geographic Manager needs additional information with regards to a program being delivered within their site, they will directly connect to the Program Manager, or their line manager.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Delegations of Authority RACI Chart (i010602)	Code of Conduct and Ethical Behaviour (e210007)
Delegations Register (i010601)	Corrective Action Plan (i011104)

5.0 GOVERNANCE

Document Owner	Chief Executive Officer	Approval Date	5 November 2021
Effective Date	25 November 2021	Document Number	i011100_v2_211125

(Uncontrolled when printed)

1.4.16 Learning and Development

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) recognises the contribution its workforce makes to the delivery of STEPS programs and services to its customer and the community. Ensuring the STEPS workforce has the capability to deliver those programs and services in an effective, efficient, and compliant manner is critical to their success.

STEPS is committed to continuous improvement by providing learning and development opportunities to its workforce that align to organisational values and goals. Further, it is also recognised that having a capable workforce includes a requirement for both technical and behavioural capabilities to meet performance expectations.

The specific purpose of this procedure is to provide a clear and transparent framework for identifying gaps in capability, providing access to Learning and Development opportunities to improve capability, and embedding improved capability and knowledge sharing across the organisation to leverage all learning and development activities accessed under this procedure, whilst meeting legislative requirements.

2.0 RESPONSIBILITIES

Executive Leadership Team will:

- Demonstrate a commitment to the learning and development of STEPS' workforce.
- Ensure the equitable provision of opportunities for employees to learning and development activities.
- Allocate the financial and other required resources to deliver learning and development activities.

Executive Managers will:

- Ensure compliance with mandatory learning and development activities.

- Minimise disruption to the delivery of day-to-day services/program requirements and learning and development activities.

Line Managers/Supervisors will:

- Proactively build the capability of their team/s.
- Identify and facilitate access to the appropriate learning and development resources/activities to improve their workforce capability and develop future workforce capability.
- Liaise with Human Resources for coordination of relevant learning and development programs.
- Roster workers to attend mandatory and compulsory learning and development activities.

Workers will:

- Objectively acknowledge their own capability, identify gaps, and seek out learning and development activities to improve their capability.
- Be accountable for meeting the capability requirements for their role.
- Participate in learning and development activities that have a direct relationship with the capability requirements for their role.
- Undertake all mandatory and compulsory learning and development activities as a worker with STEPS.

3.0 WORKFORCE CAPABILITY

Workforce capabilities refer to the required skills, knowledge, and behaviours for a task. Building workforce capability is about ensuring that workers have the capability requirements to meet short and long-term business goals. Capabilities can be both technical and behavioural, they are measurable and are set across the organisation in a variety of ways, including:

- Role Descriptions.
- Policies and Procedures, including the Code of Conduct and Ethical Behaviour (e210007)
- Job Safety Environmental Analysis (JSEA).
- Legislation/regulatory requirements.

3.1 IDENTIFYING REQUIRED CAPABILITIES

To determine the required capabilities managers/supervisors should consider:

- Strategic objectives,
- The operating environment (including possible changes),
- Achievement of performance objectives, and
- Employee’s goals and interests.

The following processes provide the opportunity for discussion and detailing capability requirements and ways to build capability:

- Probation reviews.
- Feedback and consultation.
- Performance Review process.
- Specific incidents/issues.

- New service contract/program.
- Strategic Workforce Planning activities.

3.2 MEASURING IMPROVED CAPABILITY ACROSS STEPS

It is critical to workforce sustainability that learning, and development programs provided and accessed under this procedure provide a demonstrated result in improved capability for the worker or workforce involved. This may be measured through the following activities (but not limited to):

- Improved customer outcomes.
- Increased customer retention.
- Improved service levels.
- Improved audit results.
- Increased compliance.
- Successfully gain new contracts/programs.
- Reduced performance gaps/issues.
- Reduction in workplace incidents.
- Reduction in employee grievances.
- Improved retention and succession for critical roles.
- Increased internal promotion.

4.0 STEPS LEARNING AND DEVELOPMENT PROGRAMS

STEPS offer a range of internal and external learning and development programs each year. Some of these are scheduled at an organisational, stream or site level and others are provided on an ad-hoc basis. These include but are not limited to:

- Mandatory Programs – required by law.
- Compulsory Programs – required by STEPS for the role or stream the worker is working in.
- Developmental Programs – optional and may be initiated by the worker or by STEPS.

The mandatory and compulsory program requirements will be reviewed by Human Resources every two years or in response to the following:

- Statutory changes.
- Changes to the operations of the business.
- Implementation of new technology or machinery.
- Risk assessments, incident investigations, inspections.
- Audit results.
- Performance Review outcomes.

The Human Resources team supports supervisors to develop and deliver identified learning and development programs internally and is also able to coordinate the provision of external providers where programs are best developed and/or delivered by an external provider due to expertise, costs, or compliance obligations.

Supervisors may also coordinate learning and development programs independently, however, the organisation recognises that it can leverage learning and development programs across the wider organisation, ensure consistency and minimise costs, where a coordinated and consultative approach is undertaken with Human Resources.

4.1 INDUSTRY/OTHER LEARNING AND DEVELOPMENT PROGRAMS

At times individuals or supervisors may identify an industry/other relevant learning and development program that would assist in developing capability for the individual or a group of individuals and/or they could be identified as a tool for reward or recognition. These may include:

- Industry Conferences, Workshops or Webinars.
- Community Forums or Networking.
- Coaching/Mentoring Programs.
- Educational Assistance, including tertiary study.

4.2 EDUCATIONAL ASSISTANCE

STEPS may agree to provide educational assistance to an employee undertaking qualifications relevant to their role that will provide skills and knowledge that will benefit the organisation.

The educational assistance is provided in accordance with the following guidelines:

- Employees to discuss their professional development plan during the annual performance review process or as professional development opportunities arise with their manager/supervisor. Managers/supervisors can approve as per the Delegations of Authority RACI Chart (i010602)
- Employees may be granted study leave of one day per subject up to a maximum of four days per year. Such leave will be included on the application form and will be approved in accordance with the application process.
- All professional development certificates of completion to be uploaded to licences or documents ConnX. Qualifications are to be uploaded to licences or documents in ConnX.

4.3 COSTS ASSOCIATED WITH LEARNING AND DEVELOPMENT PROGRAMS

- **STEPS Learning and Development Programs** – Supervisors have an allocation for learning and development activities and wages for attendance in their budget and this should be utilised for carrying out their responsibilities under this procedure.
- **Industry/Other Learning and Development Programs** – All workers wishing to access industry or other relevant external learning and development programs can apply for financial support, which could include costs for such programs being fully funded or partially funded by STEPS.

4.4 APPROVAL FOR ATTENDANCE AT LEARNING AND DEVELOPMENT PROGRAMS

- **STEPS Learning and Development Programs** - attendance at organisational learning and development programs will be approved by the workers’ supervisor.
- **Industry/Other Learning and Development Programs** – attendance at industry or other relevant learning and development programs will require endorsement by the worker’s supervisor but final approval will be made by the relevant manager as per the Delegations Register (i010601)

4.5 OUTCOMES FOR PROCEDURAL BREACH

Where a worker refuses to participate in learning and development programs, specifically those that are considered mandatory or compulsory, this may lead to disciplinary action and will be dealt with under the Managing Underperformance (e220300) and Disciplinary Action and Effective Termination Procedure (e210600).

5.0 RECORD KEEPING

All learning and development programs delivered will require an Attendance Register (i070201) be completed which will be saved and filed electronically ('O' Drive) by the Department conducting the training.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Attendance Register (i070201)	Role Description *(available from HR Department)*
Code of Conduct and Ethical Behaviour (e210007)	Delegations Register (i010601)
Study Assistance Application Form (i070202)	Delegations of Authority RACI Chart (i010602)
Disciplinary Action and Effective Termination Procedure (e210600)	Managing Underperformance (e220300)

7.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	5 July 2022
Effective Date	20 July 2022	**Document Number**	i070200_v3_220720

(Uncontrolled when printed)

1.4.17 Leave

1.0 INTRODUCTION

In order to assist all employees to maintain a healthy work life balance, STEPS Group of Companies (STEPS) aims to support employees by providing access to appropriate leave arrangements.

1.1 DEFINITIONS

NES	National Employment Standards

2.0 ANNUAL LEAVE

2.1 ANNUAL LEAVE ACCRUAL

Full-time employees and part-time employees (on a pro rata basis) are entitled to annual leave.

Casual employees are not entitled to annual leave.

Annual leave accrues on a daily basis. Employees can access annual leave entitlements as they accrue.

Annual leave entitlements will be paid out on separation of employment.

2.2 ANNUAL LEAVE REQUESTS

All requests for annual leave must be made through the Human Resources Information System, ConnX.

Annual leave will only be paid where an entitlement to such leave exists. Any approved request in excess of the entitlement will require approval by the Managing Director in exceptional circumstances.

Requests for annual leave should be made in a reasonable time prior to the start of the leave period. A minimum of two weeks’ notice must be provided by STEPS Community Support Services employees. The busier times of the year (school holidays and Christmas/New Year period) will require at least six weeks’ notice for consideration by the manager/ supervisor.

Changes to approved annual leave are made through ConnX. The manager must ‘rescind’ the leave application and then the employee resubmits a new leave application.

2.3 ANNUAL LEAVE APPROVAL

Leave will be approved at the discretion of the manager/supervisor with the following considerations:

- Operational needs of STEPS (i.e. the needs of the organisation, clients and the capacity of remaining employees to absorb any additional work)
- The manager/supervisor will take into consideration that all employees within the department or site will have fair and equal access to approved leave during peak holiday periods.
- The manager/supervisor will consider any extenuating or special circumstances.

Annual leave must be approved prior to taking leave.

Employees will be notified of the outcome (approval or non-approval) of their leave application via an email generated by ConnX.

2.4 CHRISTMAS/NEW YEAR CLOSURE

Various areas of STEPS close between Christmas and New Year holiday period, depending on business requirements. Employees are expected to reserve enough annual leave to accommodate this period, if applicable.

If an employee has not accrued sufficient leave to accommodate the closure over the holiday period, an application for advancement of Annual Leave may be made in exceptional circumstances to the Managing Director for approval.

Where an employee is required by their manager/supervisor to work on any of these days over the closure, the manager/supervisor and employee will agree to an alternative day/s leave.

STEPS Community Services employees are not permitted to pre-book consecutive peak holiday periods such as Christmas and Easter. This is to ensure a fair and transparent process where client's needs are met and whether the employee has worked the peak holiday period the year prior are taken into consideration. Christmas leave requests must be lodged in October for review and outcomes advised in November.

2.5 ANNUAL LEAVE CONDITIONS

To achieve a healthy work life balance employees are encouraged to have an annual leave balance of less than the annual entitlement (e.g. four weeks).

The manager/supervisor may direct an employee to take annual leave:

- if the employee has accrued an excessive amount of paid annual leave
- during STEPS' shut down between Christmas and New Year.

2.6 ILLNESS AND/OR INJURY WHILST ON ANNUAL LEAVE

Where an employee suffers from illness or injury whist on annual leave and a medical certificate can be provided, hours will be deducted from their personal/carer's leave balance (if available) for the unfit period noted on the medical certificate and credited to the annual leave balance.

2.7 PAY OUT OF ANNUAL LEAVE

All requests of payout of annual leave will be considered in extenuating and exceptional circumstances by the Managing Director, as STEPS encourages a healthy work/life balance for its employees.

Any approved payout will require the employee to retain an entitlement to at least four weeks paid annual leave (as per the NES).

3.0 PERSONAL/CARERS LEAVE ACCRUAL

3.1 PERSONAL/CARERS LEAVE APPROVAL

Full-time employees and part-time employees (on a pro rata basis) are entitled personal/carer's leave.

Casual employees are entitled to unpaid personal/carer's leave.

Personal/Carer's leave accrues on a daily basis. Employees can access personal/carer's leave entitlements as they accrue.

Paid personal/carer's leave is cumulative but will not be paid out on separation of employment.

3.2 PERSONAL LEAVE APPROVAL

Paid personal leave is available to an employee when they are absent due to personal illness or injury.

Employees must advise by telephone as soon as possible when unavailable to attend work due to illness or injury. Employees must contact their manager/supervisor directly to seek approval for access to personal leave. If employees are having difficulties contacting their manager/supervisor they must contact their next manager/supervisor directly for approval. Employees must advise of their inability to attend for duty and as far as practicable stating the nature of the injury, illness or emergency and the estimated duration of the absence. If an employee has not contacted their manager/supervisor or next manager/supervisor prior to their normal start time, disciplinary action may be taken.

All requests for personal leave must be made through ConnX within three days of returning to work.

3.3 CARER'S LEAVE APPROVAL

The entitlement to use personal leave for the purposes of carer's leave is subject to the person being either:

- a member of the employee's immediate family; or
- a member of the employee's household (as defined in the NES).

The term immediate family includes:

- Spouse, de facto partner, child, parent, grandparent, grandchild, sibling, or child, parent, grandparent, grandchild or sibling of the employee's spouse or de facto partner; and
- Child or an adult child (including an adopted child, a stepchild or an ex-nuptial child), parent, grandparent, grandchild or sibling of the employee of the spouse of the employee.

When taking leave to care for members of their immediate family or household who are sick and require care and support, or who require care due to an unexpected emergency, the manager/supervisor must be advised by telephone of:

- the name of the person requiring care and support and their relationship to the employee
- the reasons for taking such leave; and
- the estimated length of absence.

Employees must advise their manager/supervisor by telephone of their inability to attend for duty. If an employee has not contacted their manager/supervisor or next manager prior to their normal start time, disciplinary action may be taken.

Personal Carer's leave is subject to the employee being responsible for the care and support of the person concerned. In normal circumstances an employee is not entitled to take leave for this purpose where another person has taken leave to care for the same person.

3.4 MEDICAL CERTIFICATE

Where an employee is absent for three or more consecutive days or exhibits a regular pattern of absence on either side of a weekend, public holiday or leave period, they are required to provide STEPS with a medical certificate or statutory declaration, evidencing the illness or injury of the person concerned and confirming the illness or injury.

STEPS may also request an employee to provide a medical certificate or statutory declaration for these purposes where it considers that the employee has taken excessive personal leave.

STEPS may require an employee to be examined by an independent medical practitioner nominated by STEPS in respect of continuing illness or injury who will provide a report to STEPS, for consideration of continued employment or modified duties.

3.5 UNPAID PERSONAL LEAVE

Where an employee has exhausted all paid personal leave entitlements, their manager/supervisor may agree to approve unpaid personal leave. This is subject to the Managing Director's approval if in excess of one week.

4.0 WORKERS COMPENSATION

4.1 WORKERS COMPENSATION ENTITLEMENT

If an employee is receiving workers compensation payments, they are not entitled to personal leave.

5.0 BEREAVEMENT/COMPASSIONATE LEAVE

5.1 BEREAVEMENT/COMPASSIONATE LEAVE ENTITLEMENT

Casual employees are not entitled to any paid bereavement/compassionate leave. However, casuals are entitled to unpaid bereavement/compassionate leave.

Full-time employees and part-time employees are entitled to paid bereavement/compassionate leave to spend time with a member of their immediate family or household who has sustained a life-threatening illness or injury. This leave may also be taken after the death of a member of the employee’s immediate family or household.

Employees are entitled to two days compassionate leave each time they meet the criteria.

Employees can take compassionate leave as:

- a single continuous two-day period
- two separate periods of one day each.

7.0 LONG SERVICE LEAVE

7.1 LONG SERVICE LEAVE ENTITLEMENT

Employees are entitled to long service leave in accordance with the NES or as amended from time to time, or such other legislation (State or Federal) that provides your entitlement to long service leave in the future.

7.2 LONG SERVICE LEAVE REQUEST

Requests for Long Service Leave should be made in a reasonable time prior to the start of the leave period. The busier times of the year (school holidays and Christmas/New Year period) will require at least six weeks’ notice for consideration by the manager/supervisor.

All requests for long service leave must be made through the ConnX.

7.3 LONG SERVICE LEAVE APPROVAL

Long Service Leave will be approved at the discretion of the manager/supervisor with the following considerations:

- Operational need of the STEPS and its related entities (i.e. the needs of the organisation, clients and the capacity of remaining employees to absorb any additional work)
- The manager/supervisor will take into consideration that all employees within the department or site will have fair and equal access to approved leave during peak holiday periods
- The manager/supervisor will consider any extenuating or special circumstances.

Employees will be notified of the outcome (approval or non-approval) of their leave application via an email generated from ConnX.

Long service leave must be approved prior to taking such leave.

7.5 PAY OUT OF LONG SERVICE LEAVE

Any long service leave entitlements will be paid out on separation of employment.

7.6 ILLNESS AND/OR INJURY WHILST ON LONG SERVICE LEAVE

Where an employee suffers from illness or injury whist on long service leave and a medical certificate can be provided, hours will be deducted from personal leave balance (if available) for the unfit period noted on the medical certificate.

8.0 LEAVE WITHOUT PAY

8.1 REQUESTS FOR LEAVE WITHOUT PAY

All requests for leave without pay in excess of one week will be at the discretion of the Managing Director.

9.0 JURY SERVICE LEAVE

9.1 JURY SERVICE DEFINITION AND REIMBURSEMENT

An employee shall notify the employer as soon as possible of the date upon which the employee is required to attend for jury service and shall provide the employer with proof of this attendance, the duration of such attendance and the amount received in respect of such jury service. The employee must return to work as soon as practicable after the employee is dismissed from jury service (unless otherwise approved this is expected to be the next working day).

10.0 COMMUNITY SERVICE LEAVE

10.1 COMMUNITY SERVICE LEAVE ENTITLEMENT

Employees will be entitled to Community Service Leave in accordance with the NES.

11.0 NATURAL DISASTER LEAVE

STEPS supports employees that may be affected by emergencies caused by natural disasters; defined as a catastrophic event that is caused by nature or the natural processes of the earth, such as a cyclone, bush fire, flooding which may affect the wellbeing and safety of employees or their family.

11.1 NATURAL DISASTER LEAVE ENTITLEMENT

Full-time and part time employees (on a pro rata basis) are entitled natural disaster leave. Casual employees are not entitled to natural disaster leave.

11.2 NATURAL DISASTER SERVICE LEAVE APPROVAL – PERSONAL CIRCUMSTANCES

In the case of an employee who is prevented from travelling from his/her usual place of residence to attend duty and the manager/supervisor is satisfied that conditions precluded any such attendance, special leave of absence up to two working days per annum may be granted on full pay without this impacting other leave entitlements.

In the case of an employee who by reason of natural disaster are required to return home before the end of their normal working hours to ensure:

- their own safety
- the protection of their family or property

- availability of transport facilities, which may later be disrupted or discontinued because of weather conditions leave of absence on full pay shall be granted for the remainder of such day.

In the case of an employee who, though able to attend their place of employment, advises that because of rising flood waters or an imminent bushfire, must of necessity remain at home to safeguard his/her property, and the manager/supervisor is satisfied that the absence is essential for that purpose, special leave of absence up to two working days per annum may be granted on full pay without this impacting other leave entitlements.

In the case of an employee who is absent from his/her usual place of residence on approved leave or during a weekend and, due to a natural disaster, is unable to return in sufficient time to attend his/her normal place of employment special leave of absence up to two working days per annum may be granted on full pay without this impacting other leave entitlements.

The maximum natural disaster leave which may be granted in any calendar year on full pay will be two days. This entitlement does not accrue and is not paid out upon departure from STEPS.

Requests for leave beyond two days will be considered relevant to individual circumstances, weather conditions etc. Any approved natural disaster leave beyond two days would be approved leave without pay, alternatively the employee may elect to take annual leave for any leave beyond two days.

In the case of an employee taking leave for the purpose of a natural disaster, the employee will indicate this leave type as Natural Disaster Leave in ConnX.

11.3 NATURAL DISASTER SERVICE LEAVE APPROVAL - STAND DOWN AS A RESULT OF A NATURAL DISASTER

The following conditions shall apply in the case where attendance at the normal place of work is not required as the employee cannot be usefully employed as a result of a natural disaster or any stoppage or work by any cause for which the employer cannot reasonably be held responsible.

In the event of the above, the expectation is that the employee continues to be available for company business and will discuss options with their manager/supervisor.

An employee who is stood down under this clause in excess of two weeks without undertaking any company business may elect to terminate his/her employment without notice and will be entitled to receive any monies due at the time of termination.

12.0 CULTURAL AWARENESS CONSIDERATION

12.1 CULTURAL AWARENESS CONSIDERATION

Managers/Supervisors will acknowledge and consider cultural diversity for employees who reasonably require absence from the workplace to meet cultural responsibilities, through a leave without pay arrangement, taking into consideration business requirements of STEPS.

12.2 CULTURAL AWARENESS LEAVE APPROVAL

Cultural Awareness Leave will be approved at the discretion of the manager/supervisor considering operational need of STEPS and its related entities (i.e. the needs of the organisation, clients and the capacity of remaining employees to absorb any additional work).

13.0 STUDY LEAVE

13.1 STUDY LEAVE ELIGIBILITY

Following approval of a Study Assistance Application Form (i070202) as part of the Learning and Development Procedure (i070200), Study Leave of one day per subject with a maximum of four days per calendar year, or as negotiated with the relevant Manager, may be approved. The study leave should be entered into ConnX as ‘Approved Study Leave’.

14.0 PAID FAMILY AND DOMESTIC VIOLENCE LEAVE

14.1 PAID FAMILY AND DOMESTIC VIOLENCE LEAVE ENTITLEMENT

Employees are entitled to Paid Family and Domestic Violence Leave (FDVL) in accordance with the NES. The entitlement is for all employees including part-time and casual employees and is for 10 days in a 12-month period. The leave entitlement will be 10 days upfront, meaning it will not accumulate over time. The leave renews on the anniversary date of the employee and does not accumulate.

Payment of the entitlement will be in accordance with the NES. Full-time and part-time employees can take FDVL at their full pay rate for the hours they would have worked if they weren't on leave.

Casual employees will be paid at their full pay rate for the hours they were rostered to work in the period they took leave.

An employee's full pay rate is their base rate plus any:

- incentive-based payments and bonuses
- loadings
- monetary allowances
- overtime or penalty rates
- any other separately identifiable amounts.

14.2 PAID FAMILY AND DOMESTIC LEAVE APPROVAL

Employees must advise their manager or supervisor of the need for FDVL as soon as practicable and include how long they expect their leave to last. This may happen after the leave has started. Employees will also need to complete the Family and Domestic Violence Leave Application (e210501) and attach required evidence, as soon as possible on return to work. The manager or supervisor may choose to facilitate the completion of the leave application for the employee if they are unable to access systems. Managers and supervisors are to forward all requests for FDVL and associated evidence to Human Resources.

If an employee is on another type of paid or unpaid leave at the time of requiring FDVL, the employee is no longer on the other form of paid leave and is taking FDVL instead. The employee may need to give their manager or supervisor the required evidence as outlined in section 14.3.

14.2 PAID FAMILY AND DOMESTIC LEAVE EVIDENCE REQUIREMENTS

The manager or supervisor can ask their employee for evidence that shows the employee took the leave to deal with family and domestic violence. If the employee doesn't provide the requested evidence, they may not get FDVL.

The evidence has to convince a reasonable person that the employee took the leave to deal with the impact of family and domestic violence.

Types of evidence can include:

- documents issued by the police service

- documents issued by a court
- family violence support service documents, or
- a statutory declaration.

Managers and supervisors can ask employees to provide evidence for as little as one day or less off work.

Managers and supervisors must take reasonably practicable steps to keep any information about an employee's situation confidential when they receive it as part of an application for FDVL. This includes information about the employee giving notice that they're taking the leave and any evidence they provide. Managers and supervisors are not prevented from disclosing information if:

- it's required by law, or
- it's necessary to protect the life, health or safety of the employee or another person.

15.0 WELLNESS DAYS

15.1 A Wellness Day is specifically geared toward relaxing, recharging and reconnecting, providing a much-needed break to pause, regroup and come back to work feeling refreshed.

15.2 WELLNESS DAY GUIDELINES

- All full-time and part-time employees have the option to convert two (2) personal leave days to two (2) Wellness Days each financial year.
- A sufficient Personal leave balance must be accrued in order to convert to Wellness Days.
- Wellness Days are not in addition to a personal leave entitlement. The days taken are subtracted from an employee's personal leave balance.
- Wellness Days cannot be 'banked' for the future, therefore if an employee decides to not take time off as Wellness Days before the end of the financial year, the benefit for that year is forfeited.
- Wellness Days are not to be taken the day before or after a long weekend.
- Wellness Days are not to be taken at the beginning or end of annual leave.
- Only one (1) Wellness Day is to be taken at a time.
- If the taking of a Wellness Day creates a hardship within the team (for example, a number of team members are already on leave, or a work deadline is business critical), the immediate supervisor has the authority to require this day off to be rescheduled.
- This benefit should be taken as a full day off, for both full-time and part-time employees. No other increments of hours are allowed, i.e. cannot be split over multiple days.
- A leave application is required to be submitted and approved via ConnX by selecting 'Personal Leave' leave type, then choosing 'Wellness Day'.

- Cashing out of Wellness Days is not permitted.
- Untaken Wellness Days are not paid out on termination of employment.
- Casual employees, labour hire or contractors, are not eligible for this benefit.

16.0 RELATED DOCUMENTS

Document Name	Document Name
Learning and Development Procedure (i070200)	Study Assistance Application Form (i070202)
National Employment Standards (NES) https://www.fairwork.gov.au/employee-entitlements/national-employment-standards	Family and Domestic Violence Leave Application (e210501)

17.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	5 October 2023
Effective Date	17 October 2023	**Document Number**	e210500_v5_231017

(Uncontrolled when printed)

1.4.18 Managing Underperformance

1.0 INTRODUCTION

The purpose of this procedure is to describe the elements of management of underperformance within STEPS and provide a process to help and encourage all employees to achieve an immediate and sustained improvement in specified areas of their role in the workplace.

1.1 DEFINITIONS

Underperformance	Underperformance is the failure to meet role expectations with agreed targets and timeframes
Unsatisfactory Performance	Unsatisfactory Performance is the same as Underperformance.
Performance Improvement Plan	The Performance Improvement Plan (PIP) is designed to facilitate constructive discussion between an employee and his or her

(PIP)	manager/supervisor and to clarify the work performance to be improved.
Misconduct	Underperformance is not the same as misconduct. Misconduct is behaviour such as, but not limited to, breach of the Code of Conduct and Ethical Behaviour, damage to STEPS' reputation, theft or assault which may warrant instant dismissal. In cases of misconduct, managers/supervisor will refer to the Effective Termination Procedure to manage the situation accordingly.

2.0 PRINCIPLES

- STEPS' Anti-Discrimination and Equal Employment Opportunity Policy, equity and diversity principles and practice underpin decision making, daily operation and management of professional relationships. Managing diversity is about creating an environment in which everyone can achieve his or her full potential.
- STEPS accepts that occasionally an employee's performance may require improvement to achieve an acceptable standard. The primary purpose of this procedure is to establish a fair and consistent process for managers/supervisors and employees to work together to improve the performance of the employee.
- The managing underperformance process differs from the Performance Appraisal Plan (PAP) process in the amount and quantity of the detail. Assuming an employee is already participating in the PAP process, the format and the expectation of the performance improvement area(s) should enable the manager/supervisor and the employee to communicate with a higher degree of clarity about specific expectations.

3.0 PROCEDURE

3.1. MANAGING UNDERPERFORMANCE

- Minor problems with performance can be dealt with informally through discussion and advice and will not result in action being taken under this procedure. Discussing unsatisfactory performance informally may lead to acknowledgement of issues such as:
    - Insufficient/inadequate skills, abilities and knowledge
    - Working environment or personal issues
    - Differences with a manager or colleague
    - Unclear goals and expectations
    - Little or no feedback between the employee and manager/supervisor
- If unsatisfactory performance problems arise there is no need to wait for the formal performance review process. It is crucial that any issues be resolved early as the longer under performance is allowed to continue, the more difficult a satisfactory resolution becomes.
- The Manager/Supervisor will arrange a meeting to outline performance concerns, summarising under performance areas with detailed examples and expectations of

immediate and sustained improvement. If improvement is gained, there is no need to undertake a PIP.

- If there is little or no improvement from the informal meeting arrangement, communication is provided to the employee stating that a performance improvement process is being initiated (via email, file notes from meeting, Outlook invite).
- The Manager/Supervisor will provide the employee with adequate notice of the Performance Improvement Plan (PIP) meeting, including date and time, the matter for discussion, and inform the employee they may bring a support person if they choose. However, the employee does not have the right to use a solicitor or other legal representative at the meeting. A witness/scribe may be present to listen and assist the Manager/Supervisor in note taking
- In all cases, consultation with the Executive Manager - Human Resources to review the communications and Performance Improvement Plan (PIP) is highly recommended. This will contribute to consistent and fair treatment of employees across the organisation.
- Non-compliance with objectives in the PIP may place continued employment in jeopardy.
- All documentation and information collected and recorded as part of the Managing Underperformance process will be documented and placed on the employee file.
- In exceptional cases, STEPS reserves the right to dispense with some or all of these stages of the procedure.

3.2. FORMAL PERFORMANCE IMPROVEMENT PLAN MEETING

- The Manager/Supervisor should consider possible communication barriers (e.g. cultural pride) in giving feedback to employees and mitigate the risk of undue anxiety. The Employee Assistance Program (EAP) is available to assist the employee to develop strategies to deal with underperformance.
- This PIP formal meeting provides an opportunity for the Manager/Supervisor to ensure the employee has a clear understanding of the expectations of the position and has the skills and knowledge to perform the required task.
- At the PIP formal meeting, the employee is to be informed of the concerns about their performance and be given an opportunity to make comments and/or present any relevant information in relation to the concerns raised.
- Agreed actions, targets and timeframes will be set and recorded on the PIP (using the Performance Improvement Plan Template) which will assist the employee to fully understand the performance standard required and when such a standard is to be attained and maintained.
- Where it is considered that the employee does not have the required skills or knowledge to be able to meet the standard of performance required and the employee would benefit from training or coaching, then training or coaching will be noted on the PIP with an expected completion date.
- Regular meetings will be undertaken (normally weekly) over a specified period of time to provide feedback and encouragement on performance and monitor the expected performance improvement.
- The Manager/Supervisor will advise the employee that they may bring a support person to the performance improvement plan completion meeting. However, the employee does not

have the right to use a solicitor or other legal representative at the meeting. A witness/scribe may be present to listen and assist the Manager/Supervisor in note taking.

3.3. SUCCESSFUL COMPLETION OF PERFORMANCE IMPROVEMENT PLAN (PIP)

- Upon the completion of the PIP, the employee will continue on with their annual Performance Appraisal Plan and continue to maintain their performance.

3.4. UNSUCCESSFUL COMPLETION OF PERFORMANCE IMPROVEMENT PLAN

- If the Manager/Supervisor has deemed the completion of the PIP unsuccessful, and there is a continual improvement with the likelihood of targets being achieved, an extension of the PIP may be negotiated (e.g. two weeks).
- If the Manager/Supervisor has deemed the completion of the PIP unsuccessful and there has been inadequate improvement, refer to the Effective Termination Procedure.
- If the Manager/Supervisor has deemed the completion of the PIP unsuccessful due to non-participation by the employee, refer to the Effective Termination Procedure.

4.0 REFERENCES

- *Age Discrimination Act 2004 (Cth)*
- *Australian Human Rights Commission Act 1986 (Cth)*
- *Disability Discrimination Act 1992 (Cth)*
- *Equal Opportunity for Women in the Workplace Act 1999 (Cth)*
- *Fair Work Act (2009) (Cth). Part 3-1 of the Act discussed 13 prohibited grounds for discrimination as ‘General Protections’. Section 351(1) of the Act describes the discriminatory grounds protected (adverse action).*
- *Fair Work Ombudsman Best Practice Guide – Managing Underperformance*
- *Sex Discrimination Act 1984 (Cth)*
- *Racial Discrimination Act 1975 (Cth)*

5.0 RELATED DOCUMENTS

Document Name	Document Name
Anti-Discrimination and Equal Employment Opportunity Policy (i010102)	Code of Conduct and Ethical Behaviour (e210007)
Employee Assistance Program (EAP) (e230100)	Effective Termination Procedure (e210600)
Performance Review Procedure (e220200)	Performance Improvement Plan (e220301)

6.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	1 November 2024
Effective Date	7 November 2024	**Document Number**	e220300_v3_241107

1.4.19 Parental Leave

Warning: This procedure contains information regarding entitlements in the event of stillbirth or the death of a child. STEPS acknowledge that these topics may be sensitive and emotionally distressing. Support and assistance are available to all employees through our Employee Assistance Program. If you require confidential counselling or guidance, please contact Converge International on 1800 687 327.

1. INTRODUCTION/GENERAL

The purpose of this parental leave procedure is to establish a structured and supportive framework that allows employees to take time off from work to care for their newborn or newly adopted child.

This procedure outlines the rights and responsibilities of both STEPS and the employee during the parental leave period. It ensures that employees have the opportunity to bond with their child, adapt to the new family dynamic, and fulfill their caregiving responsibilities without the fear of losing their job or facing discrimination.

STEPS recognises that parental leave promotes work-life balance, employee well-being, and gender equality by acknowledging and accommodating the needs of parents in the workplace.

1.1 DEFINITIONS

Adoption-related	Means leave of either of the following kinds: • unpaid parental leave taken in association with the placement of a child for adoption. • unpaid pre-adoption leave.
Birth-related	Means leave of either of the following kinds: • unpaid parental leave taken in association with the birth of a child. • unpaid special parental leave.
Day of placement	Means the earlier of the following days:

	• the day on which the employee first takes custody of the child for the adoption. • the day on which the employee starts any travel that is reasonably necessary to take custody of the child for the adoption.
De facto relationship	Means a person is in a relationship with another person and: • are not legally married to each other, and • are not related by family, and • having regard to all the circumstances of their relationship, they have a relationship as a couple living together on a genuine domestic basis.

2. PARENTAL LEAVE ELIGIBILITY

Parental Leave is available to STEPS employees who have or will have responsibility for the care of a child. Parental leave can be taken after:

- an employee gives birth, or
- an employee's spouse or de facto partner gives birth, or
- an employee adopts a child under 16 years of age.

Generally, STEPS employees are entitled to parental leave if they have worked for at least 12 months of continuous service:

- before the date or expected date of birth if the employee is pregnant, or
- before the date of the adoption, or
- when the leave starts (if the leave is taken after another person cares for the child or takes parental leave).

Eligible casual employees are employees who have:

- been working for STEPS on a regular and systematic basis for at least 12 months, and
- a reasonable expectation of continuing work with STEPS on a regular and systematic basis, had it not been for the birth or adoption of a child.
- Labour hire casuals that convert to permanent employment are not eligible until they have worked for at least 12 months with the business entity they are employed under.

2.1 ADOPTION-RELATED PARENTAL LEAVE

An employee is entitled to adoption-related parental leave if the child:

- Will be under 16 years of age on the expected date of placement, and
- Has not lived continuously with the employee for a period of 6 months or more, and
- Is not (except through adoption) a child of the employee or the employee’s spouse or de facto partner.

2.2 PARENTAL LEAVE USAGE

The entitlement to parental leave is to a maximum of 12 months. This includes the use of Unpaid Parental Leave (UPL) and Flexible Unpaid Parental Leave (FUPL) and other relevant leave types.

3. UNPAID PARENTAL LEAVE

UPL must be taken in a single continuous period.

If the leave is birth-related, for the parent who is pregnant, parental leave can start:

- up to six weeks before the expected date of birth,
- earlier if the employee and their manager agree.
- During the 24-month period starting on the date of birth of the child.

Notwithstanding the above, UPL must end during the 24-month period starting on the date of birth of the child.

If the leave is not related to giving birth, the period of leave must start and end during the 24-month period starting on the date of birth of the child.

4. DIRECTION TO TAKE UNPAID PARENTAL LEAVE

If a pregnant employee wants to work in the six weeks before their due date, their manager may ask for a medical certificate that confirms:

- a statement of whether the employee is fit for work, and
- if the employee is fit for work, a statement of whether it is recommended for the employee to continue in their present position during a stated period because of:
  - illness, or risks, arising out of the employee’s pregnancy; or
  - hazards connected with the position.

If the certificate says they’re fit for work, but it isn’t safe for them to continue in their normal job, then the employee may be entitled to a safe job or no safe job leave if they have met the requirements of section 7 of this procedure.

STEPS can direct the employee to start UPL (excluding FUPL) if:

- The employee does not provide the certificate within seven days of the request, or
- The certificate states they are not fit to work, or
- The certificate says they’re fit for work, but it isn’t safe for them to continue in their normal job and they have not met the requirements of section 7of this procedure.

An employee’s UPL starts when they’re directed to take leave and will count as part of their total UPL entitlement.

If the employee intends to take UPL at a point after giving birth, the directed leave period does not need to be taken continuously with the rest of the parental leave.

5. FLEXIBLE UNPAID PARENTAL LEAVE

An employee can take up to 100 days of FUPL within a 24-month period starting from the child's date of birth or day of placement. The leave is unpaid and counts towards the employee's entitlement to 12 months of parental leave. The number of days of FUPL taken should not exceed the number of flexible days agreed upon with the manager. Part-time and eligible casual employees have full access to FUPL.

The employee can take the leave as a continuous period of one or more days or as separate periods of one or more days each.

A pregnant employee may take FUPL during the six weeks before the expected date of birth of the child.

The employee can take FUPL regardless of whether they have taken other UPL for the same child. However, the total duration of all periods of all parental leave must not exceed 12 months.

FUPL cannot be used to break up the continuous usage requirements of UPL as described in section 3 of this procedure.

5.1 MULTIPLE BIRTHS

If the employee has multiple children born or placed for adoption on the same day, and they have already taken FUPL for one of the children, they are not entitled to take FUPL for the other child.

6. SAFE JOBS

Pregnant employees, including casual workers, have the right to move to a safe job if their usual job poses a risk to their pregnancy. This right extends to employees who are not eligible for parental leave.

Employees wishing to seek transfer to an appropriate safe job must provide STEPS with a medical certificate that they are fit for work, but it is not recommended for the employee to continue in their present position during a stated period (the risk period) because of:

- illness, or risks, arising out of the employee’s pregnancy; or
- hazards connected with the position.

An appropriate safe job is a job that has:

- The same ordinary hours of work as the employee’s present role, or
- A different number of ordinary hours, as agreed by the employee.

If there is an appropriate safe job available, STEPS will transfer the employee to this role for the duration of the risk period, or the pregnancy ends.

If transferred to an appropriate safe job, STEPS will pay the employee at the rate of pay for the position the employee was in before the transfer, for the hours worked in the risk period.

The employee may receive different penalties and loadings while working in an appropriate safe job.

Where no safe job exists, the employee may be eligible for no safe job leave.

7. NOTICE AND EVIDENCE REQUIREMENTS

Employees must provide written notice of the intention to take parental leave at least 10 weeks before starting the leave.

7.1 UNPAID PARENTAL LEAVE

If it is not possible, notice can be provided as soon as possible (which may be after the leave commences) if the following conditions apply:

- The first period of leave taken must be UPL, or
- The leave starts before the child’s expected date of birth.

Notice must specify the intended start and end dates of the UPL. Where suitable, notification may take the form of a leave request within the HR system.

7.2 USING UNPAID PARENTAL LEAVE

Four weeks prior to the commencement of UPL, employees must confirm the intended start and end dates or advise the manager of any changes to the intended start and end dates. Where suitable, notification may take the form of a leave request within the HR system.

7.3 FLEXIBLE UNPAID PARENTAL LEAVE

If it is not possible, notice can be provided as soon as possible (which may be after the leave commences) if the leave starts before the child's expected date of birth.

If the first (or only period) of leave is FUPL, the notice may be given at any time by agreement with the manager.

Notice for FUPL is to specify the total number of days the employee intends to take in relation to the child.

With agreement of the manager, the employee may reduce the number of FUPL to zero or increase the number of days, but not over 100 days.

7.4 USING FLEXIBLE UNPAID PARENTAL LEAVE

At least four weeks' notice is needed when applying for FUPL. If this is not possible, application should be made as soon as possible (which may be after the leave has started).

By agreement, the employee may change the day notified as FUPL.

Where suitable, notification may take the form of a leave request within the HR system.

7.5 EVIDENCE REQUIREMENTS

Employees who have given notice to use parental leave must provide evidence of:

- **Birth-related leave** - the date of birth or expected date of birth of the child. Section 14 of this procedure applies for the stillbirth of a child.

- **Adoption-related leave** - the day of placement or expected date of placement of the child, and that the child will be under 16 as at the day of placement or the expected day of placement.

STEPS may require evidence for birth-related leave to be a medical certificate.

An employee is not entitled to take parental leave unless the notice and evidence requirements are met.

8. REDUCING AN APPROVED PERIOD OF PARENTAL LEAVE

By agreement, an employee whose period of parental leave has started may reduce the total number of days taken.

9. EXTENDING AN APPROVED PERIOD OF PARENTAL LEAVE

Note: Managers are required to contact Human Resources to discuss the applicability of entitlements in these circumstances before approving requests.

Employees may request an extension of UPL of up to 12 months. The extension must immediately follow the end of the available UPL.

9.1 RESPONDING TO REQUESTS TO EXTEND

The manager is to forward all requests to extend UPL to the CEO or MD as relevant. A written response is required within 21 days of receiving the request.

9.2 APPROVING A REQUEST

The response must include the following:

- All relevant details of the request, and
- STEPS approves the request, or
- STEPS approves a period of extension to an already approved request.

9.3 REFUSING A REQUEST

Requests can only be refused if the manager has:

- Discussed the request with the employee, and
- Genuinely tried to reach an agreement with the employee, and
- No such agreement could be reached, and
- The manager has had regard for the consequences of the refusal for the employee, and
- The refusal is on reasonable business grounds.

Reasonable business grounds for refusing requests may be:

- That the extension of the period of unpaid parental leave requested by the employee would be too costly.
- That there is no capacity to change the working arrangements of other employees to accommodate the extension of the period of unpaid parental leave requested by the employee.
- That it would be impractical to change the working arrangements of other employees, or recruit new employees, to accommodate the extension of the period of unpaid parental leave requested by the employee.
- That the extension of the period of unpaid parental leave requested by the employee would be likely to result in a significant loss in efficiency or productivity.
- That the extension of the period of unpaid parental leave requested by the employee would be likely to have a significant negative impact on customer service.

The written notification for a refusal for extension of parental leave must include:

- Details of the reason for the refusal, and
- State the business grounds for refusing the request, and
- Explain how those grounds apply to the refusal, and
- Either:

  - Set out the period of extension STEPS would agree to, or
  - State that STEPS is not willing to agree to any period of extension.

9.4 DISPUTES ABOUT EXTENSIONS FOR PERIODS OF PARENTAL LEAVE

A dispute may arise when STEPS refuses a request or 21 days have passed since the employee made a request and STEPS has not provided a written response.

All disputes should be raised as per the Employee Grievances procedure in the first instance.

Employees may refer the dispute to the Fair Work Commission if STEPS is unable to resolve the dispute.

10. OTHER RELATED LEAVE

10.1 PRE-ADOPTION LEAVE

Two days unpaid pre-adoption leave may be available to employees who are taking parental leave to care for an adopted or long-term fostered child to attend relevant interviews or examinations.

The employee must provide notice of leave as soon as possible (which may be after the leave has started) and must include the expected period of leave. Notice may be provided via an application for leave in the relevant HR system. Employees may be required to provide evidence of the leaves purpose.

This leave can't be used if the employee is directed by their manager to take another type of leave (for example, paid annual leave).

10.2 NO SAFE JOB LEAVE

Employees who meet the following criteria have an entitlement to paid no safe job leave:

- No appropriate safe job is available, and
- The employee is entitled to unpaid parental leave, and
- The employee has complied with the notice and evidence requirements of section 7 of this procedure.

For a full-time or part-time employee, no safe job leave is paid at the base rate of pay for ordinary hours of work that would have been worked during the risk period.

For a casual, no safe job leave is paid at the base rate of pay (not including the casual loading) for the average number of hours they would have worked in the risk period.

If an employee is on paid no safe job leave during the six week period before the expected date of birth of the child, the conditions of section 4 (direction to take UPL) of this procedure will apply.

Employees who aren't entitled to unpaid parental leave may take unpaid no safe job leave. Employees will be required to provide STEPS with evidence as outlined in section 7.5 of this procedure.

10.3 UNPAID SPECIAL PARENTAL LEAVE

Note: Managers are required to contact Human Resources to discuss the applicability of entitlements in these circumstances before approving requests.

Employees may be entitled to a period of unpaid special parental leave if they are not fit for work due to:

- The employee is pregnant and has a pregnancy-related illness, or

- All the following conditions are met:
    - The employee has been pregnant; and
    - The pregnancy ends after a period of at least 12 weeks (other than by the birth of a living child), and
    - The child is not stillborn.

Notice must be given as soon as practical, which may be after the leave has started. Employees must advise their manager of the period or expected period of the leave.

Evidence may be required for the taking of unpaid special parental leave, STEPS may request this evidence to be a medical certificate.

Where STEPS has requested evidence, the employee will not be entitled to leave until such time as that evidence is provided.

11. KEEPING IN TOUCH DAYS

Keeping in touch days allow an employee who is still on parental leave to go back to work for a few days.

11.1 WORK ON A KEEPING IN TOUCH DAY

This is a good way for employees who are caring for a baby or newly adopted child to stay up to date with their workplace, refresh their skills and assist their return to work. Work on a keeping in touch day may include:

- Participating in a planning meeting
- Doing on the job training
- Attending a conference.

11.2 NUMBER OF KEEPING IN TOUCH DAYS

An employee on unpaid parental leave gets 10 keeping in touch days. This doesn't affect their unpaid parental leave entitlement.

If the employee extends their period of unpaid parental leave beyond 12 months, they can take an additional 10 days.

11.3 WHEN KEEPING IN TOUCH DAYS CAN BE WORKED

Keeping in touch days can be worked:

- As a part day
- 1 day at a time
- A few days at a time
- All at once.

A keeping in touch day can be worked at least 42 days after the birth or placement of a child.

It can only be earlier if the employee requests it; however, if a request is made, a keeping in touch day can't be worked earlier than 14 days after the birth or placement.

The employee and manager must agree to the keeping in touch days, and an employee doesn't have to use keeping in touch days if they don't wish to.

Use of keeping in touch days does not extend the total period of parental leave beyond 12 months.

Employees will be paid ordinary hours and accrue leave when utilising keeping in touch days.

12. RETURNING FROM PARENTAL LEAVE

Employee’s returning from parental leave will return to the position held before starting the period of leave. Unless if, before starting the period of parental leave, the employee:

- was transferred to a safe job because of their pregnancy, or
- reduced their working hours due to their pregnancy.

In this case, the employee will return to the position held immediately before that transfer or reduction.

If the employee’s position no longer exists, an available position for which the employee is qualified.

UPL does not exclude STEPS from taking all reasonable measures to consult with and provide details on decisions that will have a significant effect on the employees pre-UPL position.

13. INTERACTION WITH PAID LEAVE

Employees may take other paid leave during parental leave. If the employee does, this will not break the continuity of the parental leave taken, nor does it extend the period of entitlement to parental leave beyond 12 months.

Employees will not be entitled to:

- Paid personal/carers leave (inclusive of Lifestyle Days)
- Compassionate leave unless related to section 14 of this procedure
- Community Service leave.

14. STILLBIRTH OR DEATH OF A CHILD

Note: Managers are required to contact Human Resources to discuss the applicability of entitlements in these circumstances before approving requests.

If an employee’s baby is stillborn or their child dies in the first 24 months of life, employees who would otherwise have been entitled to, can take up to 12 months’ UPL. During this time the manager or other STEPS employees must not:

- Call them back to work, or
- Cancel their unpaid parental leave.

Employees who experience a stillbirth or death of their child can choose to cancel their leave and return to work.

If the employee hasn’t started their leave, they need to give written notice cancelling the leave.

If they decide to return to work after starting their leave, four weeks written notice is required before returning. By agreement, managers and employees can agree to an earlier return date.

Employees may access compassionate leave whilst on unpaid parental leave in these circumstances.

15. HOSPITALISATION OF A CHILD

An employee who has a child that is to remain in hospital after the birth or is hospitalised immediately after the birth, may, on agreement with their manager not take parental leave for a period, while the child remains in hospital. This arrangement is known as the permitted work period.

The permitted work period is taken to not have broken a period of UPL and must start after the birth of a child. The permitted work period is taken to have ended at the earliest of the following:

- The time agreed ends
- The child is discharged from hospital after birth
- The child dies.

Employees are entitled to one period of permitted work.

STEPS may require the employee to provide evidence of one or both of the following:

- The hospitalisation of the child
- The employee is fit to work.

STEPS may require this evidence to be a medical certificate.

16. NO LONGER RESPONSIBLE FOR THE CARE OF A CHILD

Note: Managers are required to contact Human Resources to discuss the applicability of entitlements in these circumstances before approving requests.

This section applies to an employee who has taken parental leave but no longer has responsibility for the care of the child for a reason other than provided in section 14 of this procedure.

STEPS may in these circumstances, provide the employee with written notice requiring the return of the employee to work on a specific day which must be:

- At least four weeks after the notice is given, and
- Not earlier than six weeks if the employee has given birth.

17. RELATED DOCUMENTS

Document Name	Document Name
Leave (e210500)	Complying with the Australian Privacy Principles (i020700)
Employee Grievance (e210100)	

18. GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	5 October 2023
Effective Date	17 October 2023	**Document Number**	e210700_v1_231017

(Uncontrolled when printed)

1.4.20 Performance Review

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has developed this procedure to:

- Acknowledge that employees are the foundation of the organisation and that the day-to-day performance of an employee's responsibilities embodies the organisation's values.

- Recognise the intrinsic link between an employee's performance and the achievement of the organisation's objectives.

- Establish a Performance Review Process that encourages open communication between managers/supervisors and employees in order to establish and reinforce performance expectations, provide feedback and to coach and guide employees as they endeavour to meet all the required responsibilities, objectives and behaviours documented in the role description.

- Support the use of communication, coaching and training to assist an employee to improve performance. On the rare occasion improved performance is not achieved and/or maintained it may be necessary to refer to the Managing Underperformance Procedure (e220300).

This procedure applies to all permanent and specific period employees (exceeding six (6) months) upon completion of the probationary period (see Probation Procedure (e220100) across STEPS and its related entities and brands.

The performance review process is not suitable to use if there are significant deficiencies in an employee's performance or conduct. In these circumstances, please contact the Human Resource team for guidance.

2.0 PERFORMANCE REVIEW PROCESS

2.1 PERFORMANCE REFLECTION

All employees will undertake a Performance Development Review (PDR) (e220203) every twelve months. In some circumstances six-monthly reviews are provided with the opportunity for formal feedback to review the employee's performance in alignment with role requirements, and also their progress toward the achievement of the performance development goals.

A Professional Development Plan (PDP) will be developed as part of the review and will assist in establishing the performance goals and measures for the next review period. The objective of the PDP is to assist the employee to meet the requirements of their position and the goals of the organisation, by identifying opportunities for professional development in areas that would make a positive contribution to the attainment of the organisation's objectives.

2.2 PRE-DISCUSSION REFLECTIONS

To make the most effective and efficient use of the PDR conversation, employees and managers/supervisors are to complete the Performance Reflection - Employee (e220201) to assist in preparing for the conversation. To provide a supportive and fair process, managers should give employees sufficient advanced notice of the scheduled meeting and encourage them to utilise the reflection form in advance of the meeting.

The objective of the performance development conversation is to provide an opportunity for formal two-way feedback regarding the employee's achievement, challenges, areas for improvement, job-satisfaction, and engagement with their role. The Performance Development Review (e220203) should inform the structure of the conversation.

3.0 PERFORMANCE REVIEW FINALISATION

The Performance Review must be completed annually and once the discussion is complete the Performance Development Review (e220203) which includes the PDP must be signed by both parties and uploaded to ConnX for reporting purposes.

3.1 INCREMENTAL PROGRESSION

Where an increment is recommended, the Managers/Supervisors will request Incremental progression via a ConnX Request Employee Changes Form, for approval as per the Delegations of Authority and RACI Chart (i010602)

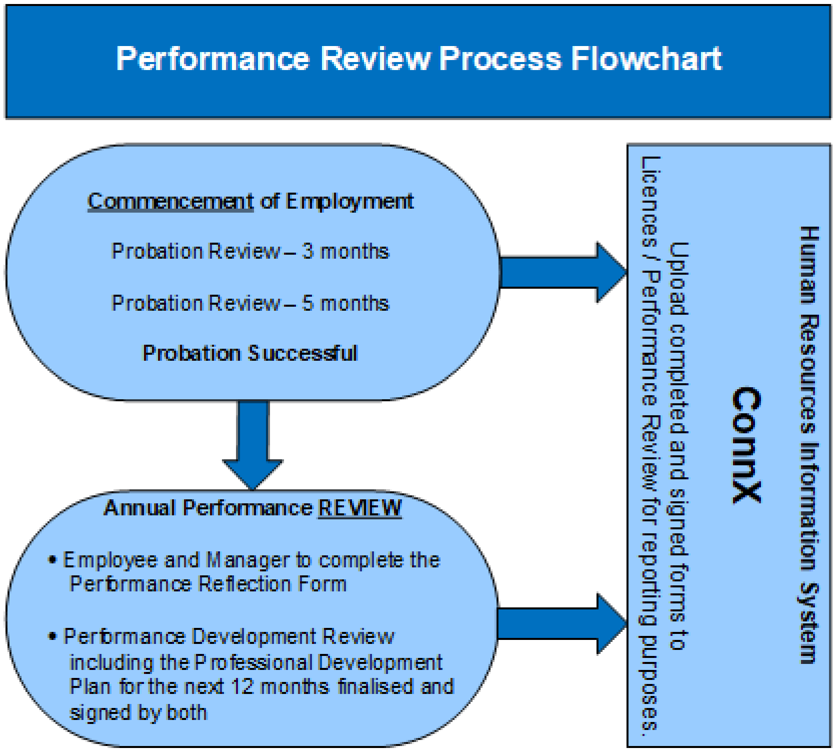
3.2 UNDER PERFORMANCE

The Managing Underperformance Procedure (e220300) is provided to help and encourage an employee to achieve an immediate and sustained improvement in specified areas of their role in the workplace.

3.3 KEY PERFORMANCE INDICATORS

Across STEPS Group of Companies there is a variation in KPI required that either could relate to the last PDR or annual KPI's. i.e. Trainers are to have their Professional Development Log up to date at the time of their PDR. Please speak with your direct line manager regarding your specific KPI's.

4.0 PROCESS MAP


Performance Review Process Flowchart
Commencement of Employment
Probation Review – 3 months
Probation Review – 5 months
Probation Successful
Annual Performance REVIEW
• Employee and Manager to complete the Performance Reflection Form
• Performance Development Review including the Professional Development Plan for the next 12 months finalised and signed by both
Human Resources Information System
ConnX
Upload completed and signed forms to Licences / Performance Review for reporting purposes.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Managing Underperformance Procedure (e220300)	Delegations of Authority RACI Chart (i010602)
Performance Development Review (e220203)	Performance Reflection - Employee (e220201)
Performance Reflection - Manager (e220202)	Probation Procedure (e220100)

6.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	19 July 2022
Effective Date	25 July 2022	**Document Number**	e220200_v4_220725

(Uncontrolled when printed)

1.4.21 Personal Information for Employees and Volunteers

1.0 INTRODUCTION

STEPS is committed to treating the personal information we collect from our employees in accordance with the Australian Privacy Principles (APPs) in the Privacy Act 1988 (Cth) (the Act). This Statement sets out how we handle employee personal information and should be read in conjunction with STEPS' Privacy Policy (i010106) and the Complying with the Australian Privacy Principles (i020700).

1.1 DEFINITIONS

Word	Definition
Employees	Any staff engaged by STEPS.
Volunteer	A person who gives time willingly for the common good and without financial gain.
Personal information	A range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Personal information can include name, signature, address, phone number or date of birth, employee record information, photographs and voice print and facial recognition biometrics.

Sensitive information	Information about a person’s race, gender diversity, sexual orientation, disability, ethnic origin, political opinions, health, religious or philosophical beliefs and criminal history.
STEPS, we, us, our	Any entity carrying out business in Australia as part of the STEPS Group of Companies.

1.2 SCOPE

This Statement applies to all STEPS employees and volunteers.

1.3 PERSONAL INFORMATION WE COLLECT

The types of personal information we collect may include:

- General identification information such as names, date of birth and gender.
- Contact details such as address, email address and phone number.
- Educational qualifications.
- Information contained in identification documents such as passport or driver’s licence.
- Government-issued identification numbers such as tax file numbers.
- Financial information such as bank account details and superannuation information.
- Visa or work permit status and related information.
- Information about immigration status.

It may be necessary for us to collect some sensitive information about you. We will only collect and use sensitive information with your consent, in accordance with applicable laws or in a de-identified aggregated manner. When collecting sensitive information, we will notify you of the reason for the collection and how this information will be used.

You might need to provide to us personal information about other individuals (i.e. emergency contacts). In these circumstances we rely on you to have informed those individuals that you are giving their personal information to us, and you have the necessary authority to provide that personal information to us. We rely on you to have advised them about this Statement and STEPS’ Privacy Policy (i010106).

1.4 COLLECTING PERSONAL INFORMATION

Generally, we collect your personal information from you directly, for example, when completing your onboarding paperwork and when you send us correspondence (including via email).

Sometimes we will collect your personal information from outside sources or a third party. For example, we may collect your personal information from:

- Your referees,

- From law enforcement agencies, or
- Education or other institutions or professional organisations.

In the collection of your personal information, we may engage third party providers, products or services who will deal with your personal information in accordance with their own Privacy Policy. You can review those websites to view a copy of the relevant Privacy Policy. In considering the use of a third party, the Outsourcing Procedure (6001000) governs the performance of due diligence undertaken by STEPS prior to engagement.

1.5 HOLDING PERSONAL INFORMATION

We may hold personal information in both hard copy and electronic formats. In some cases, we engage third parties to host electronic data on our behalf. For example, when documents and forms of identification are scanned using STEPS ICT infrastructure the data contained on those items is retained and stored by external service providers in the cloud.

We take security measures to protect the personal information we hold which includes physical controls [refer to the Physical Security Procedure (6001200) as well as technological controls [refer to the Network Security Procedure (6000900)].

We also have policies and processes which govern document retention and data breach incidents. We endeavour to ensure that personal information is kept as current as possible, and that irrelevant or excessive data is deleted or made anonymous as soon as reasonably practicable. However, some personal information may be retained for varying time periods to comply with legal and regulatory obligations and for other legitimate business reasons.

1.6 PURPOSE FOR COLLECTING, HOLDING, USING AND DISCLOSING PERSONAL INFORMATION

We will only use your information if we have a lawful reason to do so, such as when it is our legal duty, if we have your consent and when it is in our legitimate interest to do so. Reasons include:

- In accordance with the terms of your employment agreement including any related reasons such as payroll, tax, and superannuation.
- For recruitment purposes such as pre-employment screenings, contacting referees, processing applications and background checks.
- To enable your access to specific program related software, e.g. Workforce Australia for Providers of Employment Services .
- Providing internal services or benefits to our staff.
- For governance and compliance purposes such as:
  - Managing quality, conduct or risk management issues such as conflict of interest.
  - Meeting regulatory obligations.
  - Where we are required to, or authorised by legislation or industry code, direction or standards to do so.

- Where evidence of compliance is required for the purposes of your employment or volunteering obligations with us (i.e. driver's licence or Working With Children Card), their handling will be in accordance with Annexure A.
- Where evidence is required to be viewed during regulatory audits with a member of the Human Resources team present.

For development and analytics purposes to develop our organisational knowledge and know how including:

- Benchmarking purposes,
- Quality assurance and thought leadership, and
- Other purposes related to our business.

We may also use non-personal, de-identified and aggregated information for several purposes including for data analytics, submissions, thought leadership and promotional purposes. Any data is anonymised or aggregated so that no personal information or information relating specifically to you is reasonably identifiable.

1.7 SHARING OF PERSONAL INFORMATION

We may share your personal information with other parties including:

- Your authorised referees and emergency contacts.
- Personnel within STEPS and our professional advisors.
- Third parties contracted by us that assist us with providing and improving our business processes, products and services.
- Nominated superannuation funds.
- Other parties including government or regulatory bodies (for example, the Australian Taxation Office), professional or industry bodies or agencies, as part of an engagement or as required by or in accordance with any industry code or industry standard.
- Other parties when you ask us to do so or when you consent to that disclosure.

In some cases, the organisations that we may disclose your personal information to, may be located in other countries such as the UK. Where we do this, we require these parties to take appropriate measures to protect that information and to restrict how they can use that information.

1.8 EMPLOYMENT REFERENCE REQUESTS

All requests for employment references will be handled by Human Resources. For information on how reference requests will be handled, refer to the Employment Reference Procedure (e340500).

1.9 ACCESS TO PERSONAL INFORMATION

It is important that you make sure the personal information we hold about you is accurate, up to date and complete. If any of your details change or if you believe that any personal information STEPS has collected about you is inaccurate, you can access this information via ConnX to update or correct any details. Alternatively, you can contact the Human Resources team (hr@stepsgroup.com.au) and they will take reasonable steps to correct the information in accordance with the requirements of the Act.

2.0 MONITORING AND SURVEILLANCE

STEPS undertakes network monitoring as outlined in the Acceptable Use Policy (6001700).

3.0 COMPLAINTS

You can notify us of any complaint you may have about our handling of your personal information by contacting the Human Resources team (hr@stepsgroup.com.au), via the Employee Grievance Procedure (e210100) or by following the Complaints Procedure (i040500).

4.0 UNAUTHORISED DISCLOSURE OF PERSONAL INFORMATION

The unauthorised use or disclosure of personal information may result in disciplinary action up to and including termination of employment.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Acceptable Use Policy (6001700)	Complaints Procedure (i040500)
Complying with the Australian Privacy Principles (i020700)	Confidential Data Procedure (6000200)
Data Breach Identification and Reporting (i020500)	Employee Grievance Procedure (e210100)
Employment References Procedure (e340500)	Information Security Incident Management Procedure (6000600)
Network Security Procedure (6000900)	Outsourcing Procedure (6001000)
Physical Security Procedure 6001200)	Privacy Policy (i010106)
Records Management Archiving (i020300)	Reference Requests Procedure (e340500)

6.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	24 June 2024

Effective Date	5 July 2024	**Document Number**	e340400_v1_240705

(Uncontrolled when printed)

ANNEXURE A

Item	Hold	Sight	Record	Monitor	Notes
Vaccination information	X		X	X	Where there is a course or program delivery requirement.
NDIS Worker Screening / Check or NDIS Endorsement		X	X	X	For employees or volunteers based in QLD and NT.
	X		X	X	For employees or volunteers based in TAS.
Working With Children card or Registration to Work with Vulnerable People		X	X	X	For employees or volunteers based in QLD and NT.
	X		X	X	For employees or volunteers based in TAS.
Driver's Licence	X		X	X	Where listed as a mandatory requirement of the role.
		X	X	X	SmartTrack.
Working rights documentation	X				For all employees or volunteers.
	X		X	X	For employees or volunteers who hold a VISA.

1.4.22 Preventing and Responding to Bullying and Harassment

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to promoting courtesy, trust and respect to a working environment that is free from workplace bullying and harassment. STEPS finds workplace bullying and harassment unacceptable and will not tolerate it under any circumstance.

1.1 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Provide the resources to ensure that all workers and customers, participants and students are aware of the Workplace Bullying and Harassment Policy (i010105) and it's supporting procedures.
- Ensure that Line Managers/Supervisors participate in regular education provided on how to deal with allegations of bullying and harassment in the workplace and applying these procedures.

Line Managers / Supervisors will:

- Educate workers regularly on the Workplace Bullying and Harassment Policy (i010105) and its supporting procedures.
- Identify and address conduct that may constitute workplace bullying or harassment by following these procedures to provide a seamless link between reporting, investigating and determining solutions for workplace bullying and harassment matters.
- Take seriously and respond promptly, impartially and confidentially to allegations of workplace bullying or harassment.
- Where a complaint is made by a worker, follow the Employee Grievance Procedure (e210100) and apply it in a robust, objective manner, based on seeking resolution, seeking support and escalating to relevant ELT member and Human Resources (HR).
- Where a complaint is made by a customer, participant or student, follow the Complaints Procedure (i040500) and apply it in a fair, prompt and confidential manner, with no retributive action towards them as their complaints and feedback will be making a positive contribution towards assisting us improve our services and supports.
- Protect complainants making a complaint and/or have been a witness to workplace bullying or harassment from victimisation.
- Undertake performance management activities and disciplinary matters through the application of reasonable management action and the Disciplinary Action and Effective Termination Procedure (e210600) and Managing Underperformance Procedure (e220300), seeking support and escalating to relevant ELT member and HR.

Workers will:

- Maintain a professional and courteous relationship with colleagues, supervisors and customers, participants and students in the workplace.
- Undertake training on workplace bullying and harassment during induction and on a regular basis (e.g. annually).
- Report any conduct that may constitute workplace bullying or harassment, including where they have directly witnessed or overheard such conduct.
- Participate in any of the procedures required to deal with an allegation of workplace bullying or harassment.
- Maintain confidentiality and privacy in relation to all matters discussed as part of a workplace bullying and harassment investigation.

1.2 DEFINING WORKPLACE BULLYING OR HARASSMENT

Workplace Bullying	Repeated and unreasonable behaviour directed towards a worker or a group of workers that creates a risk to health and safety. **Repeated behaviour** refers to the persistent nature of the behaviour and can refer to a range of behaviours over time. **Unreasonable behaviour** means behaviour that a reasonable person, having considered the circumstances, would see as unreasonable, including behaviour that is victimising, humiliating, intimidating or threatening.
Cyberbullying	Is bullying conducted with the use of technology, like mobile phones or the internet.
Harassment	Involves unwelcome behaviour from another worker (or group of workers) that intimidates, offends or humiliates a person because of a particular personal characteristic such as those listed below: • race, (including colour, descent or ancestry, nationality, national or ethnic origin); • age (whether young or older); • impairment (including biological, functional, learning, physical, sensory, mobility, cognitive, psychological, psychiatric impairment or the presence of an organism capable of causing disease); • religious belief or activity; • sex or gender identity; • relationship status (including being married, single, divorced, separated, de facto or in a same sex relationship); • sexuality; • pregnancy, breastfeeding, parental status (including being or not being a parent, guardian, foster parent, adoptive parent or step parent); • family responsibilities (including the responsibility to care for and support a dependent child or immediate family member); • lawful sexual activity as a sex worker; • trade union activity; • political belief or activity; or • Association with someone else who is identified because of one of the above attributes.
Sexual Harassment	Any form of unwelcome sexual attention that might offend, humiliate or intimidate the other person.

2.0 IDENTIFYING BULLYING?

2.1 BEHAVIOURS THAT DO NOT CONSTITUTE BULLYING OR HARASSMENT

Reasonable management action is not bullying or harassment. Reasonable management action is that taken by Supervisors to direct and control the way work is carried out and is not considered to be workplace bullying or harassment if the action is taken in a reasonable and lawful way.

A number of behaviours do not constitute workplace bullying, including:

- Constructive feedback or counselling on work performance or work related behaviour that is intended to assist workers to improve their work performance or the standard of their behaviour; or
- Critical comments indicating performance deficiencies
- Maintaining reasonable workplace goals and standards
- Asking a worker to perform reasonable duties in keeping with their job.

Bullying and harassment can occur between a supervisor and a worker, between co-workers, or between a worker and a customer, participant or student, or between customers, participants and students.

Indicative behaviours that may constitute bullying or harassment include:

- assault, pushing or unwanted physical contact;
- yelling, screaming, swearing or abuse;
- personal insults or threats;
- inappropriate comments about appearance or slandering family members;
- offensive jokes, spreading malicious rumours or practical jokes;
- tampering with personal effects or work equipment;
- public reprimands or belittling;
- constant criticism or trivial fault finding;
- ostracising and isolating an worker;
- deliberately over-working or under-working an worker;
- deliberately withholding work related information;
- excessive supervision;
- singling out and treating one worker differently from other workers; or
- Inappropriately threatening the loss of employment or a cut-back in work hours.

3.0 STRATEGIES TO PREVENT WORKPLACE BULLYING AND HARASSMENT

STEPS aim to prevent and eliminate workplace bullying and harassment by:

- providing general training to all employees and management aimed at eliminating workplace bullying or harassment;

- implementing a Code of Conduct and Ethical Behaviour (e210007) to govern the workplace behaviour of all workers;
- informing all workers of the overarching policy and these procedures;
- regularly reviewing the overarching policy and this procedure, grievance procedures and training of all workers; and
- Consistently reporting bullying or harassment and investigating allegations.

STEPS also aims to prevent and eliminate bullying and harassment in the service environment by talking about the following where appropriate (e.g. at service entry or during enrolment or orientation):

- the value of diversity with the community and understanding that each individual is unique and brings with them individual differences that should be values and respected,
- STEPS policy on bullying and harassment and the complaints procedure to report bullying, emphasize that the sooner bullying is reported and action is taken the sooner things can change.
- Talk about bullying before it happens, through discussion on work health and safety, explanation of handbooks, lessons and other activities.
- providing the Factsheet on Cyberbullying
- When talked about in a lesson provide students with opportunities to learn and practice effective strategies for responding if they are bullied and if they see bullying happen to someone else

All employees who feel that an incident of workplace bullying or harassment, as defined in the guidelines below, has occurred should follow the Employee Grievance Procedure (e210100). All other workers/customers should follow the Feedback and Complaints Policy (i010103).

4.0 RESPONDING TO A BULLYING OR HARASSMENT COMPLAINT

If a complaint of bullying or harassment is received by a customer, participant or student follow the Complaints Procedure (i040500) and report to the line manager / supervisor immediately.

On receipt of a complaint about workplace bullying or harassment, the line manager / supervisor will review this procedure and the definitions for workplace bullying and harassment.

The supervisor will then initiate the Employee Grievance Procedure (e210100) or the Complaints Procedure (i040500) where practical. If this is not practical, they will immediately report the matter to the relevant ELT member and/or HR.

Through the application of the Employee Grievance Procedure (e210100) or the Complaints Procedure (i040500) should it be substantiated that workplace bullying or harassment has occurred; the Line Manager / Supervisor will take appropriate disciplinary action according to the Disciplinary Action and Effective Termination Procedure (e210600) and Managing Underperformance Procedure (e220300) or in accordance with the contract and expectations established for the customer, participant or student.. These measures will depend on the nature and circumstance of each breach and could include:

- a verbal or written apology;
- one or more parties agreeing to participate in counselling or training;
- in the case of customer, student or participant, suspension or ending service provision, and
- for employees, disciplinary action (such as; formal warning, transfer, demotion or suspension), up to and including termination of the worker/s engaging in the bullying or harassing behaviour.

If it is not substantiated that workplace bullying or harassment has occurred but that there has been other workplace issues identified, the Line Manager / Supervisor and/or relevant ELT member will take appropriate action to address any identified workplace issues, involving HR, where required.

The Line Manager / Supervisor will advise the complainant of the outcome of any reported workplace bullying and harassment complaint.

4.1 RESPONDING TO CYBERBULLYING

Workers, customers, participants and students can protect themselves online or on their phone by following the strategies below:

- Do not retaliate and do not respond when angry or upset.
- Give phone numbers to friends only.
- Use ID blocking on your phone to hide your number when you call others.
- Think before you send a text message or make a call.
- Keep records of calls or messages that are offensive or hurtful.
- Don't share your passwords, not even with friends. Things change, even good friendships.
- Social media is a public space. Don't post anything you really wouldn't want others to see or know about.
- Treat your friends and others how you would want to be treated.

4.2 REPORTING CYBERBULLYING

If a customer, participant or student is experiencing cyberbullying suggest that they:

- Report it – the Office of the eSafety Commissioner website has information and direct links to social networks and online gaming websites reporting pages.
- Look for a Report abuse button if you are on social networking sites.?
- If you feel physically threatened, call the police in your state or territory.
- Block, delete or report anyone who is harassing you online.
- For more information about online safety issues and what you need to know to protect yourself, go to the Office of the eSafety Commissioner website.

4.3 EMPLOYEE SUPPORT

STEPS provides an Employee Assistance Program (EAP) to all employees which provides access to professional and confidential counselling services for work-related or personal issues in accordance with the Employee Assistance Procedure (e230100). Any employee involved in a workplace bullying or harassment matter is encouraged to access these services through the EAP.

4.4 RECORD KEEPING

All records in relation to the reporting and investigation of a workplace bullying or harassment complaint should be stored in a confidential file with HR.

All records in relation to any disciplinary outcomes should be stored on the employees file, according to the Disciplinary Action and Effective Termination Procedure (e210600) and Managing Underperformance Procedure (e220300).

4.5 UNRESOLVED WORKPLACE BULLYING AND HARASSMENT

If the issue is not resolved through this procedure and application of the Employee Grievance Procedure (e210100), workers can contact the following government bodies:

- *Fair Work Australia*;
- *Workplace Health and Safety Queensland or the relevant state regulator; and*
- *Australian Human Rights Commission or the relevant state body.*

5.0 RELATED DOCUMENTS

Document Name	Document Name
Code of Conduct and Ethical Behaviour (e210007)	Disciplinary Action and Effective Termination Procedure (e210600) *plus Supporting Documentation*
Employee Assistance Procedure (e230100)	Employee Grievance Procedure (e210100) *plus Supporting Documentation*
Feedback and Complaints Policy (i010103)	Complaints Procedure (i040500)
Feedback Procedure (i040100)	Managing Underperformance Procedure (e220300) *plus Supporting Documentation*
Workplace Bullying and Harassment Policy (i010105)	

6.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	4 May 2023
Effective Date	12 May 2023	**Document Number**	i050700_v4_230512

(Uncontrolled when printed)

1.4.23 Probation

1.0 PURPOSE

The purpose of this procedure is to affirm STEPS Group of Companies (STEPS) commitment to probation as a means of ensuring new employees settle into their positions, meet role expectations and become productive from the commencement of employment with STEPS. These probation procedures are designed to create engagement and contribute to the retention of new employees.

1.1 DEFINITIONS

Probation	A defined period of time during which a new employee’s performance is subject to formal reviews. During this time, the employee is provided with clear job expectations, continuing constructive guidance, regular feedback and support to confirm progress and/or identify difficulties and develop strategies for their resolution.
Probation period	A six month period (based on calendar months) from the date of commencement of employment where the supervisor assesses the suitability of the employee for the role and the employee has an opportunity to determine if the role meets their needs.

1.2 RESPONSIBILITIES

Executive Leadership Team and the Program Managers will:

Demonstrate an integrated approach to developing and reviewing employee performance within the probation period.

Work with Human Resources (HR), who will develop, maintain and review probation tools, resources and activities to support overall engagement with new employees.

Supervisors will:

- Conduct probation activities utilising the resources developed by HR and the relevant department to ensure consistency and compliance.
- Provide regular and timely feedback to employees on their performance and address performance issues as they arise.
- Complete the Probation Reviews for new employees in accordance with the required timeframes and ensure the documentation is uploaded to the HR Information System, ConnX.
- Ensure compliance with mandatory induction training requirements during the probation period.

Employees will:

- Actively participate in probation activities and complete the Probation Review documentation within the required timeframes.
- Raise any concerns regarding their employment with their supervisor in the first instance.
- Be accountable for meeting the capability requirements for their role within a reasonable timeframe, following commencement.
- Complete induction and training activities that have a direct relationship with the capability requirements for their role.

2.0 PROBATION REVIEW PROCESS

All new employees (except casuals) have a six month probationary period. For Trainees employed under a registered training contract, the probation period stipulated in the training contract will apply.

In undertaking probation activities, the following will occur:

- Within the first two weeks of the new employee's commencement, the supervisor will meet with the new employee and discuss the Probation Review Plan (e220101). During this meeting, the supervisor will discuss the role expectations and behavioural requirements as stated in the Role Description and identify any training required to be completed during the probation period. At this time, the supervisor will schedule all required Probation Review Meetings with the employee.
- The supervisor will provide informal feedback regularly to the employee on their performance during the probation period. Formal Probation Review meetings will occur prior to the end of the third month and the fifth month of the probationary period (at a minimum). ConnX will issue reminders to supervisors.
- At the final Probation Review, the supervisor will confirm successful or unsuccessful probation completion. HR will provide formal notification to employees advising of their successful completion of the probation period.
- All probation reviews are to be uploaded into the Licenses section of ConnX.

2.1 SUPPORT FROM HUMAN RESOURCES

HR offers advice, support and assistance to supervisors and employees throughout the probation process. A HR representative will contact the employee after one month to conduct an interview regarding their onboarding experience.

Supervisors who have any concerns regarding the performance of a new employee during the probation period are to contact HR as soon as these issues arise.

2.2 UNSUCCESSFUL PROBATION

Where an employee is deemed not to have successfully completed the probationary period, employment will not be continued. Before the employee is notified, the supervisor must contact HR (at least three business days prior to termination) and seek the relevant approvals as per the Delegations Register (i010601).

The employee will be notified in writing and given one weeks' notice of termination of employment. After the employee has been notified the supervisor is required to complete a Request to Terminate Employee workflow form in ConnX and follow exit procedures.

3.0 RECORD KEEPING

All probation documentation, including file notes, should be recorded in ConnX.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Probation Review Plan (e220101)	Delegations Register (i010601)
Role Description *(refer to Human Resources Department)*	Employee Exit Procedure (e210300)

Performance Review Procedure (e220200)	

5.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	4 May 2023
Effective Date	12 May 2023	**Document Number**	e220100_v3_230512

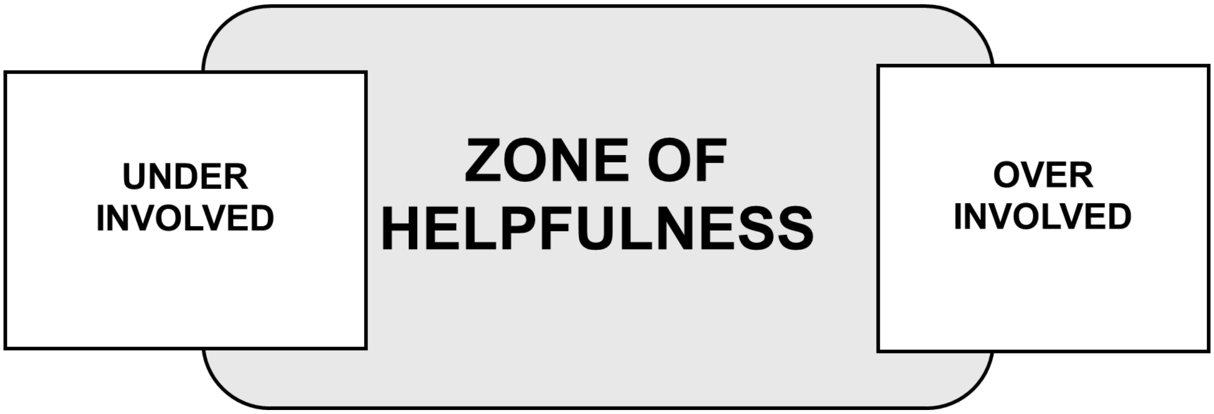
(Uncontrolled when printed)

1.4.24 Professional Boundaries

1.0 INTRODUCTION

Workers will need to provide specific services to participants. To do so effectively, workers are required to know a series of definite boundaries beyond which it is inappropriate to go.

A Continuum of Professional Behaviour



A zone of helpfulness is the centre of the professional behaviour continuum. This is where professional interactions should occur for optimal effectiveness and participant safety. Under-involvement can include distancing, disinterest and neglect. Over-involvement includes boundary crossing and violations.

1.1 DEFINITIONS

Participants	Participants are:

	• A Client/Student/Participant/Learner in a STEPS program such as Education and Training, Community Support, NDIS, Employment, Pathways College and Mental Health Programs. Those who experience a severe and persistent mental illness, psychiatric disability, challenging behaviours, intellectual disability and/or dual diagnosis and who receive services from STEPS. • For the purposes of this procedure, the scope of "Participants" shall also include students enrolled in STEPS' Education and Training services
Professional Behaviour	**Professional Behaviour is:** • Consistent conduct and behaviour that convey respect for the dignity of participants and others.
Professional Boundary	**A professional boundary is:** • A clearly established limit of conduct and behaviour that allows for safe and constructive connections between participants and their service providers; and • A clear understanding of the limits and responsibilities of a service provider's role.

2.0 ORIENTATION

2.1 All workers will receive an introduction to the Professional Boundaries Procedure during orientation outlining their professional role prior to employment commencing.

2.2 Discussions will be held with workers around:

- How the relationship between the participant and the worker is not one of equal balance by the very nature of the participant's diagnosis. However, the rights and needs of the participants must always be respected.
- Workers needing to recognise and understand that they are in a position of power and that this must not be abused at any time. All interactions between workers and participants must be seen in terms of a professional relationship.
- Workers having a clear framework within which they are to carry out therapeutic interactions. As there is potential for their position of power to be abused and professional boundaries broken, workers need to understand that the responsibility to maintain such boundaries rests with them.
- Workers ensuring that working relationships are not misread or confused with friendship or other personal relationships. This is essential to protect participants at a time when they may be vulnerable and to protect workers from the risk of potential allegations.

- If workers are ever in doubt or require clarification around professional boundaries, they are to seek advice from their Manager.

3.0 ACTIONS OUTSIDE OF PROFESSIONAL BOUNDARIES

Below are actions that could be considered to be outside of STEPS' Professional Boundaries. This list is not exhaustive:

3.1 Disclosing to a participant something personal or intimate about you that may change the participant's perception of you, leading them to believe that the disclosure implies a special trust.

3.2 If you had an undisclosed personal relationship with a participant before becoming the participant's service provider.

3.3 If you have a personal relationship with a participant either after you have ceased being a service provider or after the participant has left the service.

3.4 Where you have established a personal relationship with the participant that has given them the expectation of you visiting them outside your shifts or appointments, attending social or sports functions together or 'dating'.

3.5 Offering personal or persuasive insights into spiritual and religious beliefs, including leaving booklets, magazines or DVDs for the participant to utilise.

3.6 Speaking or acting in a flirtatious or sexual manner implying a sexual attraction to the participant.

3.7 Any form of sexual conduct or contact.

3.8 Providing adult DVDs, sexually explicit magazines or books.

3.9 Providing alcohol or cigarettes or purchasing them for a participant, unless this has been explicitly endorsed by the participant's support team.

3.10 Gossiping or disclosing information or feelings about other participants, your employer or other workers.

3.11 Offering a denigrating opinion or observation about events, other people or family members.

3.12 Assisting a participant with putting on or removing clothing unless this is part of your role description (outer layers such as a jacket, jumper or socks).

3.13 Assisting a participant with personal hygiene unless this is explicitly endorsed by the participant's support team.

3.14 Providing a participant with your own or other service provider's personal telephone numbers, email address, social media contact, address or other personal contact details.

3.15 Taking a participant to your home, family or friends' homes, private functions or other social activities of a personal nature except where this has been explicitly endorsed by the participant's support team.

4.0 BREACHES TO PROFESSIONAL BOUNDARIES

4.1 Failure to meet this responsibility may result in a worker facing a range of responses from targeted or issue-based supervision to formal disciplinary actions, which may include termination of employment and legal action.

i100400_v1_241002

1.4.25 Recruitment and Selection

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has developed this procedure to ensure transparency, consistency, equity and alignment to the organisational values, in its recruitment and selection processes.

The Recruitment and Selection Procedure is based on the principle of merit, which means that the most suitable person for the position will be chosen by assessing an applicant's skill, ability, capacity and characteristics against those that the person must have to fulfil the requirements of the job.

1.1 DEFINITIONS

Role	A role represents the job function and responsibilities of an employee.
Position	A position is a place within the organisational structure and it is linked to a role.

1.2 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Review and approve requests to recruit, where the workforce needs have been considered and the appropriate position has been developed or reviewed to meet current and future operational requirements.
- Review and approve requests to appoint, where a recruitment and selection process has taken place that supports this procedure.
- Support supervisors with recruitment and selection decisions, as required.

Supervisors will:

- Perform the role of hiring manager for these procedures for roles that directly report to them.
- Utilise Human Resources (HR) throughout the recruitment and selection process, as required, to ensure organisational consistency and minimise any risk of exposure for the organisation in making appointment decisions under these procedures.
- Meet the requirements for record keeping, ensuring that decisions are documented in relation to the application of these procedures utilising the Human Resources Information System (HRIS), ConnX.
- Participate in education and training to effectively perform the role of hiring manager and/or participate as a panel member in selection decisions.
- Identify and report any conflict of interest that may prevent them from applying these procedures to HR.

1.3 ANTI-DISCRIMINATION AND EQUAL EMPLOYMENT OPPORTUNITY (EEO)

The Anti-discrimination and Equal Employment Opportunity (EEO) Policy (i010102) outlines STEPS commitment to a diverse workplace and seeks to create an inclusive environment that accepts each individual's differences, embraces their strengths and provides opportunities for everyone to contribute their unique experiences to the workplace. STEPS recognise its obligations under the legislation in relation to discrimination in the workplace. This legislation includes: Human Rights Commission Act 1986; Age Discrimination Act 2004; Disability Discrimination Act 1992; Racial Discrimination Act 1975; Sex Discrimination Act 1984 and relevant state legislation.

Where recruitment and selection decisions require STEPS to positively discriminate against a specific group of people to meet their contractual obligations in delivering their services, it will do so in accordance with the special measures provided for under the relevant legislation (i.e. identified/funded positions for indigenous, disabled).

2.0 RECRUITMENT AND SELECTION ACTIVITIES

The recruitment and selection process is an opportunity for STEPS to present as a professional employer and service provider to the community. It is important that at every stage of the procedures outlined, that this reputation is protected and that every applicant is provided with an experience that, whilst they may not be offered employment, they feel they were kept informed and provided a high level of service throughout the process.

The procedures for recruitment and selection involve the flexible application of the following activities:

- determining workforce needs;
- reviewing and designing Role Descriptions (RDs) and selection criteria;
- approval to recruit;
- developing and applying attraction activities;
- undertaking selection processes;

- conducting pre-employment activities; and
- completing the appointment procedures.

2.1 DETERMINING WORKFORCE NEEDS

When considering undertaking recruitment activities the hiring manager should determine workforce needs by considering the organisation's objectives, efficient use of existing resources, business requirements, delegations and budget limitations. Where it is an existing position (i.e. part of the current establishment and within the current workforce budget) the hiring manager should review current and future business requirements to determine whether the role should be reviewed to reflect those requirements (e.g. if the vacant position is currently full time, could it be a part time role, could it be based in another location etc.).

Where it is a new role, the hiring manager should liaise with the relevant ELT member and other identified stakeholders to establish the workforce need and prepare any documentation required to justify the creation of a new role being established and added to the workforce budget. Prior to proceeding to any further stages in these procedures, the hiring manager should seek approval in principal from the relevant approvers, according to the delegations. All new roles and positions require the Managing Director's approval.

In determining workforce needs, the hiring manager is encouraged to consult with HR. HR can assist with workforce planning, job design and flexible working arrangements to support any workforce changes.

2.2 ROLE DESCRIPTIONS AND SELECTION CRITERIA

The relevant manager with authority should review the current Role Description (RD) or compile a new RD (e200101 - template available from HR) where the position is new to the organisation, in consultation with the relevant ELT member. The RD should contain the main accountabilities of the position. The relevant manager with authority should consult with HR when developing new RDs or reviewing existing RDs to discuss and determine the appropriate classification level.

All draft RDs should be forwarded to HR for review and finalisation. Managing Director's approval is required for all RDs created for new roles and for changes to existing RDs where the changes are significant or they change the intent of the role.

As part of the RD development or review, the selection criteria should also be reviewed to ensure each criterion is appropriate to assess the applicants' ability to fulfil the requirements of the position. This should include any mandatory requirement or characteristics that need to be met as a genuine occupational requirement (e.g. qualifications).

Once the workforce need has been established the role requirements and responsibilities have been prepared in a RD and selection criteria developed, the hiring manager must use this information to identify how the position will be structured. This includes determining the type of employment, the term of employment, the appropriate classification under the relevant industrial instrument, desired commencement date, any additional remuneration or allowances and other items as required.

2.3 APPROVAL TO RECRUIT

Once the hiring manager has structured the position, they must seek formal approval to recruit for the role by completing the appropriate request form in ConnX.

- Approval – Recruitment Request – Existing; or
- Approval – Recruitment Request – New Position.

The completed form along with the RD and any supporting documentation required, should be submitted for approval to the relevant approvers, according to the delegations register. All new positions and existing positions where the RD has changed significantly require relevant approval through this process, up to the Managing Director.

2.4 ATTRACTION ACTIVITIES

In order to provide the best outcomes and services for its clients, STEPS is committed to attracting talent into vacant positions through a variety of methods, including:

Internal transfers, secondments or promotions

- Redeployment
- Direct appointment
- Advertising on STEPS website (Careers Portal)
- Advertising on job boards
- Recruitment agencies
- External networks
- Clients
- Social media.

STEPS is committed to promoting all vacancies (internal and external) to its internal labour market and to identifying career development opportunities within the organisation.

There are also specific situations (e.g. specialist skills, emergency casuals) that may warrant direct appointment into roles in order to meet the workforce requirements, whilst maintaining STEPS contractual obligations. All direct appointments should be clearly justified in the Appointment Recommendation process (refer to Section 4.0 of this procedure).

Advertising directly on STEPS' Careers Portal, external job boards, and on social media are the most common attraction activities. Based on previous recruitment activities and current contractual arrangements the hiring manager will determine the most suitable advertising medium in collaboration with STEPS Staffing Solutions.

In areas of skills shortages or where experience has shown that traditional methods of advertising do not attract the quality of applicants required, the hiring manager should contact STEPS Staffing Solutions to discuss other strategies.

2.5 SELECTION PROCESSES

The selection process will be focused on utilising tools to determine whether applicants meet the identified selection criteria, based on merit. This may involve a range of selection activities, including:

- short-listing applications

- interviewing applicants using interview questions (which include preferred responses and may also include practical exercises to measure competency)
- reference checking
- pre-employment medical screening.

Where it is identified that selection methods other than those outlined in the procedure (e.g. psychometric or skills testing) will assist to determine an applicant's suitability for the role, in terms of demonstrating competence, the hiring manager will liaise with STEPS Staffing Solutions to ensure they are consistent with these procedures.

The hiring manager must determine who will be involved in the selection process, which must include at least one other person (other than the hiring manager). Those involved will perform the role of a selection panel and will be responsible for assessing the applications to determine the most suitable applicant based on merit throughout the selection process.

During the selection process, the hiring manager (usually the Panel Chair) will be responsible for:

- determining what selection activities will be used to make the selection decisions;
- identifying and reporting any potential conflicts of interest in the selection process and escalating any disclosed potential conflicts of interest or prior knowledge to HR for consultation;
- liaising with applicants (via STEPS Staffing Solutions) to advise them at each stage of the process, what the stage will involve, what they are required to do and provide as part of the selection process
- responding promptly to applicant enquiries (via STEPS Staffing Solutions);
- using merit based assessment to determine which applicants will be invited to attend an interview;
- coordinating all actions undertaken by the selection panel;
- briefing the selection panel on their obligations under legislation and the requirements of STEPS policies and procedures;
- determining the format of the interview; finalising interview questions (including preferred responses) with HR;
- advising applicants who are unsuccessful at any stage of the selection process (via STEPS Staffing Solutions)
- completing the relevant documentation e.g. interview guide
- closing out all recruitment campaigns (via STEPS Staffing Solutions).

All selection panel members will be responsible for:

- obtaining a clear understanding of the requirements of the position and the selection criteria and preferred responses to interview questions/activities;
- contributing to decision making on selection activities;
- actively participating in the selection activities and completing required documentation;

- preserving the confidentiality of the selection procedures; and
- avoiding any conflict of interest and advising the hiring manager of any such situation, disclosing any prior knowledge of applicants that may adversely affect the outcome of the selection process.

2.6 SHORT LISTING APPLICATIONS

Short listing activities are designed to identify those applicants who best meet the selection criteria, based on a written application, which may include their resume, responses to the selection criteria or other documents or work samples requested on application. If a position has mandatory requirements, these may be used to screen out ineligible applicants immediately and only those applicants who satisfy the mandatory requirements will continue in the application process.

2.7 INTERVIEWING APPLICANTS

STEPS Staffing Solutions in collaboration with the hiring manager will schedule interviews with short-listed applicants, requesting mandatory documents and any special requirements to ensure reasonable adjustments are accommodated for the interview.

Prior to the interview, the hiring manager will discuss with the other selection panel members the interview format and what role each person will play. The hiring manager should familiarise themselves with the STEPS Interview Guide (e200102) and Interview Question Bank (e200106) preparing the interview questions in line with the RD, organisational fit and selection criteria, seeking support from HR at any time.

The most successful interview method is behavioural based and is the foundation of the Interview Guide (e200102). When preparing the interview questions, the key is to ensure the questions prepared are based on the key requirements of the position and are open-ended to encourage applicants to provide evidence of past performance/behaviour. There is only a limited amount of time for each interview and it is important to capitalise on making each and every question count to inform the selection decision.

During the interview process the hiring manager must advise the applicants of the remaining selection activities and pre-employment or appointment requirements.

At the completion of all interviews the selection panel is responsible for identifying the most suitable applicant/s, based on merit, to proceed to the next stage in the selection process.

2.8 REFERENCE CHECKS

STEPS Staffing Solutions will then contact the referees to complete reference checks on the applicant/s. References from a minimum of two (2) referees should be undertaken, with preference for currency and relevancy and ideally at least one should be a professional reference from a previous supervisor. Where the referee is unavailable or the information is inconclusive STEPS Staffing Solutions must contact the applicant to obtain the details for further referees.

2.9 PRE-EMPLOYMENT ACTIVITIES

Prior to recommending the appointment of the most suitable applicant the hiring manager must ensure all pre-employment requirements are satisfied and uploaded to the Appointment Recommendation form in ConnX. To determine the pre-employment requirements, the hiring manager should refer to the:

- Interview Questions (Refer to the Interview Guide - e200102)

- Role Description (RD)
- Evidence of Right to Work in Australia Matrix (e200104)
- Criminal History Checks Matrix (e200201)

Further, specific positions will be determined to require pre-employment medical screening or testing which is designed to minimise risks to an applicant if they were appointed and to the organisation in meeting its work health and safety obligations. All applicants being considered for appointment to work in a remote location will undergo pre-employment medical screening, as part of the selection process. The hiring manager will liaise with STEPS Staffing Solutions who will manage the pre-employment medical process and the results must be returned and reviewed prior to the employee commencing work. This process may take up to one week.

3.0 SELECTION DECISION

At the end of the selection activities, the selection panel should assess the applicant's performance at all stages in the selection process against the selection criteria and finally consider the pre-employment activities to determine the preferred applicant. This should determine who the offer of employment should go to and who would be selected if that applicant declines the offer.

Prior to recommending appointment and once there is a full understanding of the selected applicant's experience and qualifications, the appropriate pay point should be determined within the approved classification by the hiring manager, who will need to review the information in the relevant industrial instrument.

4.0 VERBAL OFFER OF EMPLOYMENT

STEPS Staffing Solutions makes the verbal offer to the successful applicant advising them of any of the conditions of the offer. If the applicant accepts the offer the hiring manager must submit the Appointment Recommendation form in ConnX.

5.0 APPOINTMENT RECOMMENDATION

The hiring manager must upload all of the selection documentation to the Appointment Recommendation form in ConnX and submit for approval to the relevant Approvers in accordance with the delegations. This includes any conditions relevant to the offer of employment including (but not limited to):

- pre-employment medical;
- acceptable criminal history checks; and/or
- collection of copies of qualifications and transcripts, photo ID, evidence to work in Australia, licences etc. (see interview questions).

6.0 OFFER OF EMPLOYMENT

Once the Appointment Recommendation is approved HR will prepare the formal written offer of employment and correspond directly with the successful applicant. The applicant must return the offer as soon as possible prior to commencement.

7.0 FINALISING THE RECRUITMENT AND SELECTION PROCESS

The hiring manager is responsible for ensuring confidentiality of all activities conducted in the recruitment and selection process to ensure privacy for individual applicants. The hiring manager should maintain documentation in a secured manner at all times and may only disclose information about applicants to anyone who is involved in the selection process, including the selection panel, HR and direct supervisors.

7.1 NOTIFYING UNSUCCESSFUL APPLICANTS

STEPS Staffing Solutions is responsible for keeping applicants advised of their progress at all stages in the recruitment and selection process and for further communication by email, once the successful applicant has accepted the offer of employment. This includes contacting the applicants who were unsuccessful from short-listing, advising those that attended interviews that they were not successful in their application and closing out the campaign.

7.2 RECORD KEEPING

Documentation of recruitment and selection activities is critical to demonstrate an objective and legal selection decision. It can be referred to if the selection decision ever comes into question. It also ensures transparency into the selection process and assists in complying with any legal requirements. The hiring manager is responsible for completing hard copy documentation and electronically recording the stages of the selection process. The hiring manager should apply appropriate naming protocols to each document uploaded to ConnX, indicating its relevance to each stage in the selection process to allow for easy document retrieval. All hard copy documents should be securely destroyed.

8.0 CONFIDENTIAL INFORMATION

STEPS Staffing Solutions and the hiring manager is responsible for ensuring confidentiality of all activities conducted in the recruitment and selection process to ensure privacy for individual applicants. The hiring manager should maintain documentation in a secured manner at all times and may only disclose information about applicants to anyone who is involved in the selection process, including the selection panel, HR and direct supervisors.

9.0 TRAINING

All hiring managers will be provided training and education in carrying out these procedures to meet STEPS obligations including best practice recruitment and selection activities.

10.0 RELATED DOCUMENTS

Document Name	Document Name
Role Description (RD) Template (e200101), *available from HR*	Interview Guide (e200102)
Pre-Employment Health Assessment *available through STEPS Staffing Solutions*	Evidence of Right to Work in Australia Matrix (e200104)

Criminal History Checks Matrix (e200201)	Interview Question Bank (e200106)
Anti-discrimination and Equal Employment Opportunity (EEO) Policy (i010102)	Criminal History Checks Matrix (e200201)

10.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	4 May 2023
Effective Date	12 May 2023	**Document Number**	e200100_v7_230512

(Uncontrolled when printed)

1.4.26 Remote Travel

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to providing, as far as is reasonably practicable, a safe and healthy workplace for all employees performing duties which involve travel in remote areas of Australia.

This document provides direction for the actions and behaviours required when undertaking remote travel and is applicable to all employees and volunteers across STEPS and its related entities and brands.

1.1 DEFINITIONS

Remote Travel	The Australian Taxation Office divides remote areas of Australia into two zones called Zone A and Zone B. There are also special areas within these zones. STEPS classify any travel to or from localities identified by the Australian Taxations Office as Special Areas within Remote Area Zones as “remote travel”. Generally, these are locations where there are few people and facilities, where communications are limited, and/or where access may be difficult.

2.0 PREPARING A REMOTE TRAVEL PLAN

A Remote Travel Plan, including a communication plan, must be prepared prior to undertaking any remote travel using the Remote Travel Plan (i050901) template. This plan must be prepared by the staff member conducting the travel and their manager, with reference to the following documents:

- Community Fact Sheet (site specific, maintained by manager)
- Risk Management Procedure (i050100)

Consideration should also be given to the following special conditions or issues:

- Travel into areas requiring special communication consideration such as satellite phone or two way radio communications

- Travelling distances where travel outside of daylight hours is unavoidable
- Driving on unsealed and unformed roads and potentially rough surfaces
- Travelling in areas where river and water course crossing and heavy rain events may occur
- Travelling into areas where emergency support such as police, fire, ambulance, first aid, and medical aid is not easily available
- Travelling in isolated areas where vehicle traffic is low
- Travelling to a remote location and staying overnight (or longer).

3.0 TRAINING

3.1 4WD TRAINING

STEPS recognise that employees will be exposed to driving conditions that vary extensively, and that employees may require training to recognise and manage the various risks associated with driving in remote areas.

If this training is identified as a requirement of the employee’s role a General Risk Assessment (i050105) must be conducted and based on the outcome of the General Risk Assessment (i050105) a 4 wheel drive course may be provided.

If an employee has completed a 4 wheel drive course the Certificate is to be uploaded into ConnX.

3.2 OTHER TRAINING

STEPS employees undertaking remote travel may also be required to undertake further training relevant to their role and the equipment and procedures for the location. This may include specific communication device training, emergency preparedness, conflict resolution, cultural awareness, and first aid training.

4.0 REMOTE TRAVEL REQUIREMENTS

4.1 FITNESS TO TRAVEL

STEPS is committed to staff safety and endeavours to provide resources that support the worker to fulfil their role. It is a necessary requirement of recruitment and selection that all trainers working in remote areas complete a *Pre-Employment Health Assessment Form*, (available from HR on request - e200105). Employees travelling remotely who have not completed a *Pre-Employment Health Assessment Form* (e200105) as part of contract requirements must declare their fitness for work prior to travel as per STEPS’ Fitness for Work Policy (i010104).

Any medical condition, health concerns and/or medication which may affect the employee’s ability to travel must be brought to the attention of their manager. Should medical checks be deemed necessary for the employee to perform their role, appropriate arrangements will be made by their manager in consultation with the STEPS Human Resources team.

Where there are specific inoculation requirements for visiting or residing within remote communities, STEPS will meet all necessary costs. Managers will maintain a Community Fact Sheet with up-to-date information on inoculation requirements specific to remote communities. Record of inoculations had by employees will be maintained in ConnX (only those deemed necessary to perform role).

4.2 SEA AND AIR TRAVEL

Trainers are likely to undertake water or air travel as part of their role. If a STEPS employee is doubtful as to the safety of the trip or if the STEPS employee feels there is a risk of harm, they should contact their manager to discuss any issues and determine an alternative method of transport where available.

4.3 WEATHER AND ROAD CONDITIONS

The following points must be considered by the employee undertaking remote travel and their manager prior to departure:

- Determine if the travel activity is a remote travel activity (refer to definition).
- Identify recommended travel times, road conditions and potential hazardous situations – refer to Community Fact Sheet (stored electronically and available from manager).
- Review up-to-date road conditions and weather reports for the locations where travel is to be conducted and ensure risk reduction measures are put in place to reduce any potential hazardous situations, with a General Risk Assessment (i050105) undertaken if required. Issues or potential hazards arising out of the above should be discussed, updated on the Community Fact Sheet and included on the Remote Travel Plan (i050901).

4.4 ACCOMMODATION

Accommodation types vary within communities. Accommodation options in remote communities are maintained in site specific Community Fact Sheets.

Employees will coordinate with their manager to confirm accommodation arrangements within the community. STEPS will arrange accommodation and confirm prior to departure.

4.5 MOTOR VEHICLE

STEPS will provide a suitable motor vehicle for the required remote travel activity.

Vehicle Type

When selecting a suitable vehicle STEPS will consider things such as – engine size and capacity; communications within the vehicle; air conditioning; luggage space; equipment that must be carried by the employee, and; whether petrol or diesel vehicle is required for the trip. Should an employee have concerns with the vehicle provided, they should discuss the matter with their manager prior to travel.

Vehicle Checks

For all occasions of remote travel undertaken in STEPS vehicles, the employee must complete a Remote Vehicle Inspection Form (i051001) prior to travel. If an issue or item of concern is noted, it must be recorded on the Remote Vehicle Inspection Form (i051001) and then discussed with their manager prior to commencing the trip, and alternative travel arrangements made.

The Remote Vehicle Inspection Form (i051001) must be signed by both the employee conducting the travel and their manager prior to commencement of the journey. These must be scanned and saved electronically on file.

For remote travel undertaken in hire vehicles, standard hire car checks must be complete. A Remote Vehicle Inspection Form (i051001)is not necessary.

Vehicle safety issues

If a safety issue arises part way through the trip, the employee conducting the remote travel must contact STEPS management and discuss an appropriate course of action. At all times, the safety and welfare of the employee is the priority concern in any such event.

Fuel

When the vehicle has been issued, the employee must ensure they understand the fuel requirements of the vehicle and fill the vehicle accordingly. If travelling to Indigenous communities, any additional fuel jerry cans must only contain diesel fuel. STEPS prohibit petrol, kerosene, methylated spirits and/or any other form of solvent to be taken into a community. Breach of this prohibition may lead to disciplinary action and possible termination of employment.

4.6 COMMUNICATION PLAN

The travelling employee must ensure the appropriate communication equipment is available, serviceable and operational and that a communication plan has been approved and understood by both manager and employee. This includes details on the frequency of communication, with whom, and the message to be conveyed. It is the manager's responsibility to devise this plan with the travelling employee as part of the Remote Travel Plan (i050901).

The Community Fact Sheet includes details on communication schedules and message requirements.

5.0 COMMUNICATION DEVICES

One or more of the following communication devices will be provided to each employee before commencing remote travel. Type of communication devises issued will be dependent on remote travel location and coverage considerations.

- Satellite Mobile Phone
- Mobile Phone
- Motor Vehicle GPS

5.1 MOBILE TELEPHONES

All STEPS mobile phone usage must be in line with the STEPS Mobile Device Policy (6002100).

5.2 SATELLITE MOBILE TELEPHONE

A satellite mobile telephone with inbuilt GPS will be issued to an employee travelling to remote communities where the manager deems necessary. STEPS will provide written documentation providing instruction on the use and capabilities of the satellite mobile telephone.

5.3 MOTOR VEHICLE NAVIGATION SYSTEM

STEPS employees may have access to a STEPS owned 4WD fitted with inbuilt navigation system for remote travel. Managers will provide necessary training on how to operate the navigation system before the employee commences travel.

The Motor Vehicle Navigation System does not have the capacity to be utilised for two-way communication. For all remote travel in motor vehicles with inbuilt navigation systems, an additional mobile phone or satellite phone must be utilised.

6.0 RECORDING TRAINING PROVIDED

The Manager will record all training provided to STEPS employees prior to remove travel in the Attendance Register (i070201).

7.0 CONTACT NUMBERS

Each employee will be issued with a list of contact number included in their Remote Travel Plan (i050901), relevant to the placement area in which the employee is travelling and will be working. The manager is responsible for maintaining a list of up-to-date contacts in the Community Fact Sheet.

The numbers will include:

- All necessary STEPS numbers, including direct telephone lines and mobile numbers
- Emergency services, including Police and Ambulance – direct station numbers
- Medical facilities
- Contact numbers for communities (e.g. Clinics, GBM, Police etc)
- Breakdown service providers.

8.0 CLOTHING

STEPS employees undertaking remote travel should be aware of the type of clothing required for the climate and cultural considerations in the community they are working. The relevant Community Fact Sheet should be reviewed prior to travel, particularly if there are any colours that are not allowed to be worn or that may offend persons within the community.

9.0 ALCOHOL AND DRUGS

Employees conducting remote travel must consult the relevant Community Fact Sheet to determine if the community is an alcohol free area. STEPS prohibit an employee from taking alcohol into such a community, or obtaining and consuming alcohol when in such a community. Breach of this prohibition may lead to disciplinary action and possible termination of employment.

All employees must adhere to STEPS' Fitness for Work Policy (i010104) and Drugs and Alcohol in the Workplace Procedure (i051100).

10.0 EMERGENCY PLANNING

An emergency situation can occur at any time; therefore if a STEPS employee conducting remote travel considers a situation as an emergency, they must immediately communicate their concern to STEPS management and to the local authorities. Employee safety is paramount; therefore, an employee should not hesitate to consider a situation as an emergency. It is important that an incident does not escalate.

If there is an emergency situation a WHS Incident Report (i090201) must be completed in accordance with the Incident Notification Procedure (i090200).

11.0 CONFLICT

STEPS employees must adhere to the organisation's Code of Conduct & Ethical Behaviour (e210007) and represent STEPS in a respectful manner while undertaking remote travel and visiting remote communities.

STEPS employees must avoid conflict. Any incident of threat, physical violence or other matter related to physical violence will be investigated by STEPS and may result in disciplinary action and possible termination of employment.

12.0 DURING THE REMOTE TRAVEL ACTIVITY

All employees conducting long distance travel are reminded – **Stop, Revive, Survive**

It is understood that on most occasions, the remote travel activity will be performed alone, that is, the driver will be on their own and must therefore at all times consider their own safety as a matter of priority.

Whilst driving, a mandatory break must be taken for at least 10 minutes for every two hours of continuous driving. If at any time an employee feels fatigued, tired or drowsy, or loses concentration whilst driving, a break of at least 20 minutes must be taken at the first safe opportunity. In doing so, be mindful of where this break is taken, avoiding isolated areas by seeking out the nearest service station or populated rest area. Where employees are sharing the driving, a change of driver should take place at least every two hours.

An employee must not drive for more than eight (8) hours, including rest breaks, on any one day of travel. However, dispensation may be provided by the manager if risk factors have been considered and appropriate mitigation practices documented in the Remote Travel Plan (i050901).

Night driving is generally prohibited; however, if for some reason night driving is unavoidable, the employee must contact their manager and gain permission.

In the event that an employee on remote travel fails to report in at the scheduled time, their manager must take the following actions:

- Within a 10 minute window after the scheduled report in time, attempt to contact the employee
- If contact cannot be established with the employee within 1 hour, their manager will alert the nearest emergency contact point and inform them of the situation. A plan of action should be devised between the manager and the emergency contact on how to best handle the situation. For example, contact by satellite and/or mobile phone will be made at ten (10) minute intervals for a period of up to one hour before the emergency contact point activates a search initiative.

Once the situation is resolved, and if it is determined that the employee simply failed to report in because the communication device was turned off or due to some other negligence, the employee is subject to disciplinary action along with being required to pay the costs incurred with enlisting the emergency services.

13.0 POST REMOTE TRAVEL

Upon return to base, employees must provide verbal feedback to their manager about their travel and visit to remote communities. It is important the manager updates the Community Fact Sheet with such information for future travel preparations.

14.0 RELATED DOCUMENTS

Document Name	Document Name
Attendance Register (i070201)	Code of Conduct & Ethical Behaviour (e210007)

Community Fact Sheet (Example) (i050903) (site specific)	Community Fact Sheet (Template) (i050902)
Drugs and Alcohol in the Workplace Procedure (i051100)	Fitness for Work Policy (i010104)
First Aid Procedure (i090400)	General Risk Assessment (i050105)
Health Safety and Environment Policy (i010101)	Incident Notification Procedure (i090200)
Mobile Device Policy (6002100)	*Pre-Employment Health Assessment Form (e200105)* *Available from HR Department if required*
Remote Travel Plan (i050901)	Remote Vehicle Inspection Form (i051001)
Risk Management Procedure (i050100)	WHS Incident Report (i090201)

15.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	24 June 2024
Effective Date	5 July 2024	**Document Number**	i050900_v3_240705

(Uncontrolled when printed)

1.4.27 Salary Packaging

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) offers employees access to salary packaging which may increase their take home pay and benefit their individual needs and financial circumstances.

This procedure sets out the relevant terms and conditions that are to apply between STEPS and any employee that wishes to participate in STEPS' Salary Packaging Program. This procedure should be read in conjunction with Fringe Benefits Tax (FBT) legislation and any relevant industrial instrument.

1.1 DEFINITIONS

Salary Packaging	Salary packaging is an agreement with your employer where a part of an employee's cash salary is set aside (sacrificed) for payment of other employee benefits (including for example mortgage, personal loans, rent, credit cards, superannuation etc). The benefit to employees is a reduction in income tax payable, resulting in an increase in available disposable income.

2.0 RESPONSIBILITIES

Executive Leadership Team will:

- Allocate the required resources to deliver the Salary Packaging Program.
- Support the engagement of an external provider to administer the Salary Packaging Program that provides an efficient and cost-effective service.
- Work collaboratively with Human Resources (HR), who will facilitate the internal processes associated with the Salary Packaging Program, including the coordination for delivery of information sessions on salary packaging.
- Ensure the program continues to meet the needs of the organisation and maximises the opportunities for employee participation.

Supervisors will:

- Facilitate access to salary packaging arrangements for eligible employees
- Refer employees with any queries in relation to the STEPS' Salary Packaging Program to the external provider.
- Complete the documentation associated with commencement, conclusion of employment and leave activities for employees, to ensure any salary packaging arrangements are updated, where required.

Employees will:

- Seek independent financial and tax advice before entering into or modifying a salary packaging arrangement, including establishing how the program is impacted by any Higher Education (HECS-HELP) debt and/or child support payments.
- Notify the external provider of any changes relevant to their salary packaging arrangements. This includes loans that are paid out, payments of salary packaging to be allocated to another account, change to employment status etc.
- Ensure that expenses declared are equal or greater than the amount that is allocated to salary packaging for that period.
- Complete the relevant documentation associated with their salary packaging arrangements.

3.0 STEPS SALARY PACKAGING PROGRAM

STEPS engages an external provider to administer its Salary Packaging Program. All employees will be provided with information on STEPS' Salary Packaging Program on commencement.

The approved Salary Packaging Program allows for the following items to be salary sacrificed (note that some restrictions do apply as listed in section 3.5 of the procedure):

- General living expenses e.g. rent or mortgage payments, personal loan payments, vehicle expenses including petrol and registration
- Entertainment benefits including meal entertainment (eating out), and holiday accommodation and hire expenses
- Pre-packaged holidays - where a travel company has bundled together the elements of a holiday (hotels, meals, cruise, flights, transfers) into a product that is advertised as a packaged holiday

- Laptop computers and mobile phones
- Novated vehicle leases
- Remote Area benefits (if applicable)
- Superannuation.

3.1 EXTERNAL PROVIDER

- The current external provider is AccessPay.
- STEPS shall provide the external provider with such information about the employee that is required by the external provider to administer the program.
- Salary packaging arrangements administered by an external provider are strictly a confidential matter between the employee and the external provider.
- Employees can find more information about salary packaging from the AccessPay website www.accesspay.com.au or via phone on 1300 133 697, or email customerservice@accesspay.com.au. Information is also available on the STEPS Intranet.

3.2 PROGRAM FEES

The cost of administration of the program is to be met by those employees elect to participate in it. The current fees are set by the external provider and available on their website.

3.3 CONFIDENTIALITY AND PRIVACY

- STEPS will treat all information obtained from the employee for the purposes of the program as confidential information and shall not divulge such information to any person, other than the external provider, without the employee's prior written consent (refer to the Privacy Policy (i010106).
- The obligations as to confidentiality, and any financial obligation, including the assessment of FBT survive any expiry, revocation or termination of the salary packaging arrangements.

3.4 DISCLAIMER

- STEPS do not accept any responsibility for any loss or damages of any kind, whether foreseeable or not, that may arise from participation in the STEPS’ Salary Packaging Program.
- STEPS employees (including HR and management) are not able to provide advice on the program or its benefits to individual employees.

3.5 RESTRICTIONS

- Employees within their probationary period are not eligible to enter into a Novated Lease agreement with STEPS until they have successfully completed their probationary period.
- Any Novated Lease agreements are to be approved by the Managing Director and/or the Chief Financial Officer. STEPS reserves the right to exercise absolute discretion when considering the approval of Novated Lease Agreements.
- Eligible casual employees who elect to participate must specify a percentage (up to a maximum of 50%) of their gross fortnightly income to be salary packaged. This amount may be deposited onto a salary packaging card for their benefit or reimbursed.
- Employees are not permitted to breach:

  - the grossed-up living benefit threshold (or such other limit as determined by the FBT legislation as it is amended from time to time)
  - the grossed-up Meal/Entertainment and Entertainment Hire/Leasing and Entertainment threshold.

- Employees are able to salary package laptop computers and other exempt items, however these must now be predominantly for business use in order to be exempt. A declaration is required to support this which needs to be authorised by the Executive Manager - Human Resources or Chief Financial Officer.
- Any FBT that is or becomes payable by an employee on their packaging arrangements is and remains an obligation for them to discharge. This obligation will survive any termination of employment from STEPS.

3.6 SALARY SACRIFICING SUPERANNUATION

Employees wishing to set up salary sacrificing of their superannuation should submit their request in writing to Human Resources at hr-payroll@stepsgroup.com.au. Payroll will process the authorised salary sacrificing of superannuation deductions to commence in the next pay period, or as nominated by the employee.

3.7 SALARY PACKAGING AND VEHICLES

STEPS Vehicles:

- An employee’s salary packaging amount will be affected where they have commuter or private use of a STEPS vehicle. The external provider will advise each employee in this regard.

Novated leasing of vehicles:

Employees may also enter into a lease arrangement for a car, if they were otherwise intending to purchase a vehicle, subject to the following conditions:

- The vehicle purchased must be less than ten years old; and
- The vehicle purchased must have at least a three to five star safety rating.

3.8 CHANGES TO SALARY PACKAGING ARRANGEMENTS

- Salary packaging agreements can be reviewed at any stage throughout the year, noting that any change to the existing arrangements can only relate to prospective, not current or past earnings.
- All salary packaging agreements can be reassessed when an employee’s terms and conditions change (e.g. if the employment status changes, contract hours are increased).

3.9 EFFECTS OF LEAVE ON SALARY PACKAGING ARRANGEMENTS

- Salary packaging arrangements will continue during periods of paid leave.
- Where planned unpaid leave is approved, employees must contact the external provider to renegotiate their salary packaging arrangements.

3.10 SALARY PACKAGING AND PAYMENT SUMMARIES

The FBT Reporting Year is from 1st April – 31st March. Generally the FBT legislation requires employers to record the grossed up amount of salary packaging benefits paid to or on behalf of an employee on their payment summary. This figure is otherwise known as the Reportable Fringe Benefit Amount.

3.11 RESIGNATION, TERMINATION AND OPTING OUT

- An employee may elect to conclude their salary packaging arrangements at any time subject to a minimum of fourteen days written notice being provided to the external provider, who will then notify STEPS HR accordingly.
- An employee may cease salary sacrificing pre-tax voluntary superannuation contributions by sending an email to hr-payroll@stepsgroup.com.au.
- Fourteen days after an employee's final pay subsequent to resignation or termination of employment, the external provider will return any remaining salary packaging funds to STEPS Payroll to be processed and paid to them as salary and wages (subject to income tax, as appropriate).
- On termination of employment, salary packaging may be calculated on any accrued leave entitlements. The external provider needs a minimum of one weeks' notice from the employee's nominated end date to make any changes to salary packaging arrangements for the employee's final pay.

3.12 TERMINATION OR ALTERATIONS TO THE PROGRAM

- This Salary Packaging Program may be altered, enhanced or withdrawn completely by STEPS at any time where components of the program change.
- In the event of amendments to any taxation legislation affecting salary packaging, STEPS will advise employees of such amendments and of any variation required to the package for the purpose of ensuring compliance with legislation.
- In the event that STEPS ceases to attract exemption from payment of FBT, or there is an amendment to exemption level, all packaging arrangements will be reviewed and may be terminated.

3.13 FAILURE TO COMPLY

Failure to comply with any of these procedures will result in cancellation of the employees' salary packaging immediately and employees will not be entitled to be reimbursed for benefits foregone.

4.0 RELATED DOCUMENTS

Document Name
Privacy Policy (i010106)

5.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	28 April 2022
Effective Date	3 May 2022	**Document Number**	e230200_v2_220503

(Uncontrolled when printed)

1.4.28 Staff Travel

1.0 PURPOSE

- STEPS recognises that travel can be an important aspect for carrying out business and that STEPS employees may be required to travel in the course of their duties. This procedure is to ensure travel for or on behalf of STEPS is appropriate, safe and advance the achievement of the organisation's priorities and strategic intent. It also sets out to ensure effective, efficient and consistent travel management across STEPS Group of Companies.

2.0 RESPONSIBILITIES

- MD and/or CEO will provide formal and final approval for all travel requests. CEO is responsible for approval of travel requests for SGA and SSS staff only.
- Line managers will endorse staff travel requests and seek final approval from MD and/or CEO as appropriate.
- Employees will submit travel requests to their line manager in the first instance.

3.0 BUSINESS RELATED TRAVEL

- Employees may request to engage in business related travel that may include but is not limited to:
  - Conferences, workshops, site visits, training and seminars.
  - Benefit to STEPS' business activities.
  - Does not duplicate activities of other business units.
  - Can be undertaken only after exploring alternatives to travel. (i.e. can this be done by email, phone, electronic conferencing or virtual meetings.)

    NB: Business related travel may be joined with travel for private purposes where it does not result in an additional unrecovered cost. Any additional costs will be invoiced and paid for by the employee

4.0 TRAVEL REQUESTS

- Any staff member wishing to undertake business related travel on behalf of STEPS must apply within a reasonable timeframe, when possible, to allow enough time for approval.
- When seeking approval, allow enough time for early bird registrations, flights and accommodation to be booked in a timely manner, especially during peak seasons.
- Provide as much travel information as you can, including dates, preferred flights/times, any airport transfers, anything else that may be required for your travel to assist the travel booker.
- Approval requests are to be submitted to the direct line Manager in the first instance.
- The relevant line Manager will then seek approval from the CEO or MD (only one signature needed). Refer to the Delegations Register (i010601)
- The decision to authorise or approve travel will be based on whether the intended travel is integral to the requesting traveller's work for STEPS.
- All travel is to be booked via the Manager, Executive Administration Team.

5.0 GUIDELINES FOR TRAVEL

- All business related travel is to be booked at the most advantageous price and service level.
- Airfares must utilise the most direct and logical best economy fare of the day where possible.
- Accommodation should be based on value for money, a safe and secure environment and convenience/proximity to travel location.
- Any associated costs which are not business-related (e.g. mini bar, alcohol, newspapers, magazines) are considered of a personal nature and must be paid separately by the traveller.
- If business travel has any personal travel days included, then leave should also be taken via ConnX for the personal leave part of the trip as well as cost of the personal travel to be paid by the traveller.
- Travel that is funded through external grants must comply with the terms of the external body's funding arrangements in addition to STEPS procedures.
- Employees are to exercise due and reasonable economy when purchasing meals or providing hospitality or entertainment for guests and visitors. Hospitality and/or entertainment must always have a clear business purpose.
- Accurate records of travel-related expenditure must be retained for finance purposes.
- Employees are always to act in a professional manner when traveling and representing STEPS, as per the Code of Conduct and Ethical Behaviour (e210007).
- Any request to cancel or change travel bookings is to be made through the Executive Administration Team.
- Employees must allow appropriate time to travel to and from the airport to ensure booked flights are taken.

6.0 RELATED DOCUMENTS

Document Name	Document Name

Code of Conduct and Ethical Behaviour (e210007)	Corporate Credit Cards (e310400)
Delegations Register (i010601)	Online Travel Booking Form (under construction)
Remote Travel (i050900)	

7.0 GOVERNANCE

Document Owner	Executive Assistant to the MD	**Approval Date**	5 October 2023
Effective Date	17 October 2023	**Document Number**	e350100_v1_231017

1.4.29 Student Placement

1.0 PURPOSE

STEPS Group of Companies (STEPS) recognises the importance of assisting students on placement to achieve their study goals. This procedure is designed to work in collaboration with educational or training organisations to ensure students are engaged, supervised and gain optimal outcomes for themselves and the organisation, at all stages of their involvement with STEPS.

1.1 DEFINITIONS

Student Placement	A vocational placement which provides students with the opportunity to apply the theory and skills they learned while studying in a workplace. Vocational placements that meet the definition under the Fair Work Act 2009 (the FW Act) are lawfully unpaid.
Student Placement Supervisor	The supervisor or nominated qualified contact person who liaises with the relevant placement organisation and supervises the student during their placement
Placement Organisation	The institution delivering the course which provides for the placement and is authorised under an Australian, state or territory law or an administrative arrangement of the Commonwealth or a state or territory to do so, such as universities, TAFE colleges and schools (whether public or private).

1.2 RESPONSIBILITIES

Executive Leadership Team will:

- Provide the guidance, structure and scope for how students are engaged, supervised and optimised.
- Allocate the required resources to facilitate student placements at STEPS.

Senior Leadership Team will:

- Work collaboratively with Human Resources (HR), who will facilitate student placement procedures that align to HR procedures.
- Ensure the inclusion of students, as workers, continues to meet the needs of the organisation and the students themselves and maximises the opportunities for student learning.
- Ensure all student placements are covered by adequate insurance.

Student Placement Supervisors will:

- Recognise the role of student placements as different from other forms of workers, including employees, and treat them as such.
- Provide student placements with supervision and support that enables them to apply their skills and learning.
- Ensure that any relevant criminal history checks are undertaken as per the Criminal History Checks Procedure (e200200).
- Assist in completing the necessary student placement documentation and Induction procedures.
- Follow these procedures for the supervision of all student placements.

Students engaged in a Student Placement will:

- Perform their role and meet their responsibilities, as a student placement.
- Comply with relevant policies and procedures as provided to them during Induction and over the period of their placement.
- Maintain regular communication with their Student Placement Supervisor and the placement organisation.
- Notify STEPS of any changes to their circumstances that may impact on completion of their student placement with STEPS.
- Complete the documentation associated with their student placement.

2.0 STUDENT PLACEMENT PROGRAM

2.1. SCREENING OF STUDENT PLACEMENTS

The Student Placement Supervisor will review requests for student placements (in accordance with their level of delegation) and screen potential student placements, liaising with the placement organisation to discuss expectations and learning interests of the student, as well as the requirements/expectations of STEPS.

2.2. ENGAGEMENT OF STUDENT PLACEMENTS

Once a decision has been made to engage a student placement, the Student Placement Supervisor will:

- Complete any required documentation by the placement organisation.
- Ensure the student completes the relevant Induction Checklist (i070101) as per the Induction Procedure (i070100).

- Ensure the student completes the relevant Volunteer documentation.
- Forward all relevant documentation to the Volunteer Relationship Coordinator for filing electronically.

2.3. CONCLUSION OF STUDENT PLACEMENTS

STEPS recognises that student placements have a right to end their involvement with STEPS at any time. Where STEPS are no longer able to accommodate a student placement, they will advise the student in person. Fair and transparent processes are in place for the ending of the involvement of a student placement, for whatever reason.

3.0 RELATED DOCUMENTS

Document Name	Document Name
Induction Checklist (i070101)	Induction Procedure (i070100)
Criminal History Checks Procedure (e200200)	Volunteer Management Procedure (i070300)

4.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	4 May 2023
Effective Date	12 May 2023	**Document Number**	e210400_v3_230512

(Uncontrolled when printed)

1.5 Volunteer Management

Enter topic text here.

1.5.1 Volunteer Management

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) identifies as a committed and inclusive Volunteer Involving Organisation. Building an inclusive and committed volunteer program that is flexible to accommodate all STEPS volunteer roles provides opportunity for all community members, brings different experiences and insights to STEPS, and aligns with the National Standards for Volunteer Involvement.

STEPS recognises the value of volunteers as an important part of the STEPS team that enhance the services delivered by the organisation. Volunteering is time freely given for the common good and without financial gain. It includes formal volunteering that takes place with an organisation in a structured way.

This procedure is designed to ensure that volunteers are engaged, managed, and optimised at all stages of their volunteering involvement with STEPS and provided with encouragement and recognition to demonstrate their valuable contribution.

2.0 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Provide the strategic guidance, structure, and scope for volunteers
- Allocate the required resources to manage the volunteer workers at STEPS
- Appoint a Volunteer Relationship Coordinator to coordinate the STEPS Volunteer Program with the necessary skills, knowledge, and abilities to perform this role
- Ensure all volunteers are adequately covered by insurance.

Line Managers will:

- Recognise the role of volunteers as different from other STEPS workers
- Provide volunteers with supervision and support that enables them to perform their roles and responsibilities
- Ensure the inclusion of volunteers, as workers, continues to meet the needs of the organisation and the volunteers themselves and maximises the opportunities for volunteer participation
- Follow these procedures for the management of all volunteers, upholding the rights of volunteers, whilst ensuring volunteers understand and deliver on their responsibilities, as outlined to them
- Complete the documentation associated with volunteer management to ensure compliant record keeping.

Volunteer Relationship Coordinator will:

- Respond to volunteer queries, liaising with Line Managers and Human Resources as required
- Provide a detailed role description to all new volunteers outlining their duties, responsibilities and accountabilities
- Assist all new volunteers in completing the necessary Volunteer documentation and Induction
- Work collaboratively with Human Resources (HR), who will facilitate the volunteer management procedures that align to the HR procedures for all STEPS workers. Undertake relevant criminal history checks as per the Criminal History Checks (e200200)
- Collate and report on volunteer involvement activities and statistics
- Manage and maintain volunteer involvement records, including personal and confidential information.

Volunteers will:

- Perform their role and meet the responsibilities, as a worker at STEPS
- Notify STEPS of any changes to their circumstances that may impact on their role as a volunteer with STEPS
- Complete the documentation associated with their engagement as a volunteer.

3.0 STEPS VOLUNTEER PROGRAM

3.1 IDENTIFIED PROGRAMS/SERVICES

STEPS identify a number of programs/services that benefit from the services of volunteers, including (but not limited to):

- STEPS Nursery
- STEPS Pathways Charity
- Events
- STEPS Pathways College
- Education and Training
- Employment.

3.2 PRINCIPLES

The STEPS Volunteer Program is built on the following principles:

- STEPS identifies as a committed Volunteer Involving Organisation
- Volunteering is always a matter of choice
- Engaged volunteers benefit the community, the organisation and the volunteer
- The service and undertakings performed by volunteers is unpaid
- Volunteers do not replace paid workers
- Volunteers have rights, which include the right to work in a safe and supportive environment with appropriate infrastructure and effective management practices
- Volunteers have responsibilities which include acting responsibly, being accountable for their actions to the organisation and respecting the organisation’s values and practices.

3.3 RECRUITMENT AND SELECTION

Recruitment and selection activities will ensure prospective volunteers are provided with sufficient information to make informed decisions about working with STEPS, and provide a consistent process for assessing, selecting, and placing new volunteers.

- Volunteers are recruited through a variety of methods
- Volunteers are selected based on the following factors:
    - Suitability for the services/undertaking required
    - Organisational fit
    - Motivation to volunteer
    - Availability.
- The selection process will include completion and review of:
    - Volunteer Application Form (i070303)/Volunteer Application Form - One Off Event (i070304)
    - Interview with Manager

  - Reference Checks
  - Criminal History Checks - refer Criminal History Checks (e200200).

3.4 APPOINTMENT AND COMMENCEMENT

Once a decision to appoint a volunteer has been made, the Volunteer Relationship Coordinator or Line Manager will:

- Sign the Volunteer Application Form (i070303) and ensure it is signed by the volunteer
- Provide the volunteer with the Volunteer/External Student Agreement (i070302) and Volunteer Deed of Confidentiality (i070307) and ensure they are both signed
- Ensure the volunteer completes the relevant Induction and Training as per the Volunteer/External Student Induction Checklist (i070305)
- Forward all relevant selection, appointment, and commencement documentation to the Volunteer Relationship Coordinator via email volunteer@stepsgroup.com.au.

3.5 CONCLUSION OF VOLUNTEER INVOLVEMENT

STEPS recognises that volunteers have a right to end their involvement with STEPS at any time. Where STEPS are no longer able to accommodate a volunteer, they will advise the volunteer in person. Fair and transparent processes are in place for the ending of the involvement of a volunteer, for whatever reason.

3.6 VOLUNTEER RECOGNITION

STEPS acknowledges the contribution that volunteers make to our organisation and is committed to recognising this value through a range of informal and formal activities that are appropriate to the volunteer role and respectful of cultural values and perspectives.

These recognition activities may include the following:

- Providing regular feedback and positive comments about achievements
- Celebratory occasions
- Informal chats with members of the ELT when possible
- Certificates of Appreciation/Service
- Gift cards
- Recognition of personal milestones and achievements (e.g. birthdays)
- Recognising and celebrating National Volunteer Week and International Volunteer Day.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Criminal History Checks (e200200)	Manager/Supervisor Volunteer Recruitment and Induction Process (i070306)
Role Description *(refer to Human Resources Department)*	Volunteer Application Form (i070303)

Volunteer Application Form - One Off Event (i070304)	Volunteer Deed of Confidentiality (i070307)
Volunteer Manual (i070301)	Volunteer/External Student Agreement (i070302)
Volunteer/External Student Induction Checklist (i070305)	

5.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	18 December 2023
Effective Date	2 January 2024	**Document Number**	i070300_v8_240102

(Uncontrolled when printed)

1.6 Work Health and Safety

Your Health and Safety Representatives

Heath and Safety Representatives (HSR) are elected by fellow workers. Representatives are entitled to carry out inspections and review the circumstances of workplace incidents. They are also entitled to participate in health and safety meetings. A Health and Safety Representative does not need any experience or special qualifications.

WHS Officer Contact Details:

Adrian Hayes – WHS Officer / (07) 5458 3041 / 0447 188 838

1.6.1 Asbestos Management

1.0 PURPOSE

To enable compliance to Work Health and Safety obligations for the management of asbestos, protecting the health and safety of all STEPS Group of Companies (STEPS) employees, visitors and contractors.

The presence of asbestos materials in a building does not necessarily create a health risk. While the materials are undisturbed and in sound condition, they will not generate airborne respirable fibres or create a health risk.

2.0 DEFINITIONS

Asbestos	The asbestiform varieties of mineral silicates belonging to the serpentine or amphibole groups of rock-forming minerals, including: actinolite asbestos, grunerite (or amosite) asbestos (brown), anthophyllite asbestos, chrysotile asbestos (white), crocidolite asbestos (blue) and tremolite asbestos, and a mixture that is a combination of 1 or more of these minerals.
Airborne Asbestos	Any fibres of asbestos small enough to be made airborne. For the purposes of monitoring airborne asbestos fibres, only respirable fibres are counted.
Asbestos Containing Material (ACM)	Any material or thing that, as part of its design, contains asbestos.
Asbestos Related Work	Means work involving asbestos.
Asbestos Removalist	A person conducting a business or undertaking who carries out asbestos removal work.
Competent Person	A person who has acquired, through training, qualification or experience, the knowledge and skills to carry out the task.
Friable Asbestos	Material that is in a powder form or that can be crumbled, pulverised or reduced to a powder by hand pressure when dry, and contains asbestos.
NATA Accredited laboratory	A testing laboratory accredited by the National Association of Testing Authorities (NATA), Australia, or recognised by NATA either solely or with someone else.
Non-friable Asbestos	Material containing asbestos that is not friable asbestos, including material containing asbestos fibres reinforced with a bonding compound.
Respirable Asbestos	An asbestos fibre that: •Is less than 3 microns (µm) wide. •Is more than 5 microns (µm) long. •Has a length to width ratio of more than 3:1.

Note: Products made from asbestos cement, a bonded asbestos material - include fibro sheeting (flat and corrugated) as well as some water, drainage and flue pipes, roofing shingles and guttering. Asbestos is a type of building material used in the building industry between the 1940s and late 1980s.

3.0 PROCEDURE

3.1 ASBESTOS REGISTER

An Asbestos Register will be developed and maintained for each site, owned by STEPS, that has buildings constructed prior to 31 December 2003. A request will be made to each Landlord for a copy of the Asbestos Register and Management Plan for each leased site that has buildings constructed prior to 31 December 2003.

A Record of Asbestos Registers and requests for provision of Asbestos registers will be developed and maintained.

The STEPS Record of Asbestos Register (i050801) will be kept up to date and record:

- Whether asbestos is at each site
- A link to the Asbestos Register and/or Asbestos Management Plan for each site which has an Asbestos Register and Asbestos Management Plan.
- The date when the Asbestos Register and/or Asbestos Management Plan is due for review
- The date an Asbestos Register and/or Asbestos Management Plan was requested from a Landlord.

Each Asbestos Register maintained for a site will record:

- The date, location and condition of asbestos or ACM.
- State that no asbestos or ACM is present at the site or likely to be present at the site from time to time.

Each Asbestos Register for STEPS owned sites where asbestos or ACM has been identified will be reviewed by a competent person when:

- The asbestos management plan is reviewed.
- Additional asbestos or ACM is identified at the site.
- Asbestos or ACM is removed from, disturbed, sealed or enclosed at the site.
- At least every 5 years or in conjunction with the review of relevant sites Asbestos Management Plans.

Steps will request an updated Asbestos Register for a leased site when it becomes aware of one of the above events occurring.

The STEPS Record of Asbestos Register (i050801) and the relevant site Asbestos Register will be made available to all STEPS employees, and contractors who carry out work at the site.

3.2. ASBESTOS MANAGEMENT PLANS

Relevant sites Asbestos Management Plans will be developed and maintained for each STEPS owned site where asbestos or ACM has been identified or assumed to be present. The Asbestos Management Plan may also contain the Asbestos Register. Copies of Asbestos Management Plans will be requested from Landlords for each leased site where asbestos or ACM has been identified or assumed to be present.

What is an Asbestos Management Plan?

An *Asbestos Management Plan* sets out how asbestos or ACM that is identified at the workplace will be managed, for example what, when and how it is going to be done.

An *Asbestos Management Plan* must include:

- The identification of asbestos and ACM, for example a reference or link to the asbestos register for the workplace, and the locations of signs and labels.
- Decisions, and reasons for the decisions, about the management of asbestos at the workplace, for example safe work procedures and control measures.
- Procedures for detailing accidents, incidents or emergencies of asbestos at the workplace.
- For those workers carrying out work involving asbestos, examples of consultation, information and training responsibilities provided.

An *Asbestos Management Plan* for a STEPS owned site will be reviewed when:

- Asbestos or ACM is removed from, disturbed, sealed or enclosed at the site.
- The plan is no longer adequate for managing asbestos or ACM at the site.
- A Health and Safety Representative requests a review.
- At least once every 5 years.

STEPS will request an updated Asbestos Management Plan for a leased site when it becomes aware of one of the above events occurring.

If a worker suspects the presence of asbestos or ACM in the workplace, the worker is required to:

- Inform their supervisor and Work Health and Safety Officer (WHSO) immediately.
- Evacuate and isolate the area.
- The WHSO will contact the appropriate agencies and provide guidance to those involved.
- If unsure, assume presence of asbestos.

3.3. TRAINING

Any STEPS employees with concerns where asbestos or ACM has been identified or assumed to be present at their worksite, should contact their site manager to discuss the following:

- The hazards associated with the asbestos on the site.
- The existence and purpose of the STEPS Record of Asbestos Register (i050801) and Site Asbestos Management Plan and Site Asbestos Register.
- The responsibilities of people at the site regarding asbestos management.
- The labelling of asbestos hazards.

3.4. AWARENESS BY CONTRACTORS

Any person conducting work on the site will be made aware of the presence of asbestos or ACM at the site and its location via STEPS Record of Asbestos Registers and the Asbestos Management Plan and Register for the Site and by the acknowledgement signed by the contractor prior to works being commenced. Each site must keep a printed copy of the AMP on site for provision to contractors.

It is of utmost importance that:

- Consultation occurs with the person carrying out the work and that they are aware of the potential hazards and risks associated with the task.

- All consultation and action items are documented.
- Liaison with the Principal Contractor occurs to establish that the following on-site systems and procedures are in place: Health and Safety rules, Induction for all workers – site specific, supervisory arrangements, communication, injury reporting, hazard reporting, PPE, exclusion zones, risk assessments, SWMS and JSAs.

3.5. ASBESTOS RELATED WORK

Asbestos related work must only be performed by a person holding the relevant certificate of competency:

- Friable asbestos removal.
- Non-friable (bonded) asbestos removal - CPCCDE3014A Remove non-friable asbestos.
- Asbestos Assessor - CPCCBC5014A Conduct Asbestos assessment.

4. RELATED DOCUMENTS

Document Name	Document Name
Record of Asbestos Register (i050801)	Relevant Site Asbestos Management Pans and Registers

5. GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	23 May 2024
Effective Date	27 May 2024	**Document Number**	i050800_v3_240527

(Uncontrolled when printed)

1.6.2 Consultation, Representation and Participation

1.0 WHS CONSULTATION

This procedure outlines the Work Health and Safety (WHS) consultative arrangements within STEPS Group of Companies (STEPS).

So far as is reasonably practicable, STEPS will consult with its employees who may be directly affected by matters relating to WHS and ensure consultation mechanisms and intent comply with legislative requirements.

The Work Health and Safety Act 2011 (Qld) prescribes consultative arrangements in the workplace between the employer and workers. This is partly achieved through the appointment of work health and safety staff, election of Health and Safety Representatives (HSRs) for work groups, and the establishment of a WHS Committee if requested.

STEPS has established a WHS Committee with elected HSRs and management representatives which will meet at a minimum once every three months. All WHS Committee Members are required to adhere to the Work Health and Safety Committee Charter (i040301). The Health and Safety Representative Nomination Form (i040304) has been attached to this procedure. Please consult with the WHS Officer before commencing the election process.

The duties and responsibilities of HSRs are outlined in the Health and Safety Representative Role and Function Statement (i040306). All HSR's are required to ensure they understand the obligations of this role and act in accordance with the Role Statement.

2.0 WHS ISSUE RESOLUTION

STEPS is committed to maintaining a safe and healthy working environment for all workers and visitors and will ensure that any WHS issues/complaints are dealt with in an expeditious and constructive manner.

The continuous systematic improvement of the IMS is dependent on the feedback and reporting mechanisms from employees. Employees are actively encouraged to communicate issues or concerns relating to WHS with their supervisor and WHS Officer as required. In attempting to resolve a WHS matter that may be a risk to health and safety, the WHS Officer will use the applicable health and safety consultation arrangements in accordance with the relevant legislation and or formally refer the matter to the Supervisor (refer to the WHS Issue Resolution Flowchart (i040303). Management will consider the matter and respond in a timely manner.

If the HSR reasonably believes that a site is contravening or has contravened the provision of the Work Health and Safety Act 2011 and resolution cannot be reached through normal consultation with STEPS, the HSR may choose to issue a Provisional Improvement Notice (i040305) Prior to issuing a PIN the WHS Officer must be consulted.

3.0 WHS COMMUNICATION PROCESS

Consultation is a two-way process between management and employees. STEPS will ensure supervisors:

- Listen to their workers concerns.
- Seek and share views and information.
- Consider what our workers say before making decisions.
- Act on legitimate concerns.
- Contribute to the decision making process.
- Workers consulted are advised of the outcome of any consultation in a timely way.

STEPS will consult with relevant workers when making changes that will affect their work health and safety. These will include:

- Changing work systems.
- Developing a new product or planning a new project.
- Purchasing new or used equipment or substances.
- Restructuring the business.
- Developing procedures and Job Safety Environmental Analysis (JSEA).
- Identifying hazards.
- When making decisions about ways to eliminate risks.
- When making decisions about facilities.
- When proposing change.
- When resolving safety issues at the workplace.

STEPS will consult with employees through regular staff meetings and facilitate the election of HSRs if requested.

Each department will conduct team meetings on a regularly basis. Topics at these team meetings will include but not be limited to resolving work health and safety issues within each Department/Stream as well as working towards improved standards in health and safety and continuous improvement within the IMS. Copies of the meeting minutes will be made accessible to employees.

4.0 SHARING INFORMATION AND SAFETY PROMOTION

STEPS will ensure workers have access to all relevant work health and safety information that may affect their health and safety. This will be achieved by providing employees access to the following:

- Health and safety policies and procedures.
- Technical guidance relevant to the work area.
- Legislative guidance.
- Hazard reports and risk assessments.
- Data on incidents and illnesses at the workplace.

The information will be presented in a way that can be easily understood by all workers and taking into account literacy needs and the cultural and diverse backgrounds of our employees.

STEPS is committed to safety promotion. General safety promotion exercises will be conducted regularly throughout the year. These will involve both employees and management and are designed to raise awareness of health and safety issues within the workplace.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Work Health and Safety Committee Charter (i040301)	WHS Issue Resolution Flowchart (i040303)
Health and Safety Representative Nomination Form (i040304)	Provisional Improvement Notice (i040305)
Health and Safety Representative Role and Function Statement (i040306)	

6.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	6 October 2022
Effective Date	10 October 2022	**Document Number**	i040300_v3_170411

(Uncontrolled when printed)

1.6.3 Electrical Safety

PROCEDURE: ELECTRICAL SAFETY

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has an obligation to ensure workers' health and safety while at work, an important component of which is electrical safety. Accordingly, STEPS will ensure that all electrical equipment used in the workplace is electrically safe by meeting the testing requirements for electrical equipment and assigning responsibilities for maintaining electrical safety at sites.

1.1 DEFINITIONS

Competent Person	A person who has acquired, through training, qualifications, experience or a combination of these, the knowledge and skill to carry out the task.
Electrical Equipment	Any apparatus, appliance, cable, conductor, fitting, insulator, material, meter or wire: 1. used for controlling, generating, supplying, transforming or transmitting electricity at a voltage greater than extra low voltage, or 2. operated by electricity at a voltage greater than extra low voltage; 3. operated by electricity at an extra low voltage, if the equipment forms part of an electrical installation located in a hazardous area; or 4. That is, or that forms part of, a cathodic protection system.
Electrical Safety	For a person or property, means the person or property is electrically safe.
Electrically Safe	1. for a person or property, that the person or property is free from electrica risk; and 2. for electrical equipment or an electrical installation, that all persons and property are free from electrical risk from the equipment or installation; and 3. for the way electrical equipment, an electrical installation or the works of an electricity entity are operated or used, that all persons and property are free from electrical risk from the operation or use of the equipment, installation or works; and 4. for the way electrical work is performed, that all persons are free from electrical risk from the performance of the work; and 5. for the way a business or undertaking is conducted, that all persons are free from electrical risk from the conduct of the business or undertaking; and 6. For the way electrical equipment or an electrical installation is installed or repaired, that all persons are free from electrical risk from the installing or repairing of the equipment or installation.
Personal Electrical Equipment	Electrical equipment not owned by STEPS and brought into a STEPS location and owned by a person or company.
Service Work	Work that is not amusement work, construction work, manufacturing work, office work or rural industry work. Examples include: Cleaning a motel, providing health services at a health facility, selling goods from a shop, teaching at an education facility.

Source: WHS Regulations and Electrical Safety Code of Practice 2021 – Managing Electrical Risks in the Workplace

1.2 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Establish and maintain systems to facilitate compliance with electrical safety legislation, associated Codes of Practice and applicable Australian Standards.
- Ensure that sufficient resources are allocated to ensure compliance and fully implement this procedure.

Site Manager/Program Coordinator will:

- Take all practicable action to maintain electrical equipment in an electrically safe condition.
- Ensure testing of electrical equipment and portable Residual Current Devices (RCDs) are carried out at prescribed intervals to the prescribed standard.
- Ensure electrical testing of electrical equipment is undertaken by a competent person in accordance with relevant legislation and standards.
- Ensure the competent person provides test records, and such records are saved on the network under the shared WHS folder, and notification is sent to the WHS Officer.
- If required, follow through with any Out of Service Tags attached to equipment and ensure items are either repaired or replace.

Employees will:

- Inspect electrical equipment for damage, such as leads, whenever the electrical equipment is moved.
- Report damaged electrical equipment to the Site Manager/supervisor, attach an Out of Service Tag, and complete a Hazard Report Form (i050103).
- Ensure that any personal equipment brought into the workplace is electrically safe i.e. tested and tagged or plugged/connected to a circuit that has a safety switch installed.

2.0 ELECTRICAL SAFETY PREREQUISITES

Electrical safety at STEPS sites shall be managed in the following priority:

a) Installation of safety switches on all power circuits with regular testing.

b) Testing and tagging of all electrical equipment not connected to power circuits fitted with a safety switch.

Testing electrical equipment shall be undertaken in accordance with the examples in the table below.

Site Examples	Type of Work Classification	Testing Frequency of Electrical Equipment When NO safety switch is installed	Testing Frequency of Electrical Equipment When safety switch is installed	Testing Frequency of Safety Switch
Caloundra - Head Office, Staff Kitchen, Site Offices	Office Work	5 Years	Not Required	6 month push button 2 years electrical test
Nursery, Commercial Kitchen (Caloundra), Cleaning Program	Service Work	Annual	Not Required	6 month push button 2 years electrical test
Caloundra - Training Rooms, Remote Community	Service Work	Annual	Not Required	6 month push button 2 years electrical test

3.0 ELECTRICAL EQUIPMENT

3.1 NEW ELECTRICAL EQUIPMENT

New electrical equipment is deemed to be electrically tested for the initial six months it has been put into use.

New electrical equipment that it not connected to a circuit installed with a safety switch must have a tag attached with the following:

- Date of entry to service
- Date when next test is due.
- Statement that “This appliance has not been tested in accordance with AS/NZS 3760”.

New electrical equipment that is connected to a circuit installed with a safety switch does not require a tag.

3.2 PERSONAL ELECTRICAL EQUIPMENT

Personal electrical equipment brought into the workplace must also meet the requirements of the table above in Section 2.

Examples can include:

- A slow cooker NOT connected to a circuit that has a safety switch must have a current electrical safety tag.
- A slow cooker connected to a circuit that has a safety switch does not need to have a current electrical safety tag.

3.3 OUT OF SERVICE TAGGING

If equipment is deemed defective or out of test date electrical equipment must have an Out of Service tag attached. Ensure all details on the tag are completed and securely attach the completed tag to the defective equipment in a prominent position.

The employee or worker who becomes aware that the equipment is defective will notify the Site Manager/supervisor and complete Hazard Report Form (i050103) if required.

If required, notify other employees at the site of the defective item.

The Site Manager will ensure that any tagged equipment is either repaired or replaced.

4.0 ELECTRICAL SAFETY RECORDS

The Site Manager must ensure that test records saved on the network under the shared WHS folder.

All test records must be kept for at least seven years.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Hazard Report Form (i050103)	Electrical Safety Act 2002 (Refer to 2.1.1 Legislation Register)
Electrical Safety Regulation 2013 (Refer to 2.1.1 Legislation Register)	Electrical Safety Code of Practice 2021 – Managing Electrical Risks in the Workplace (Refer to 2.1.1 Legislation Register)

6.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	06 October 2022
Effective Date	10 October 2022	**Document Number**	i080200_v1_170523

(Uncontrolled when printed)

1.6.4 Emergency Planning

1.0 PLANNING FOR EMERGENCIES

This procedure provides guidance on planning, documentation, and communication of Emergency Management for all STEPS Group of Companies (STEPS) workers and applies to all STEPS workplaces.

STEPS adopts a multi-faceted approach to emergency planning that includes:

- Emergency management to safeguard people from harm by taking actions during and immediately after a crisis occurs
- Business Continuity which aims to maintain or restore key business operations or services (internally and externally) to its pre-crisis state.

1.1 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Provide adequate resources to ensure this procedure is implemented within STEPS
- Conduct regular reviews of risk assessments, emergency management plans and continuity plans.

Line Managers/Supervisors will:

- Ensure that all workers in their area of responsibility are aware of, and understand, the content and application of this procedure
- Ensure site inspections and training for all workers occur as scheduled. Ensure that Emergency Wardens undertake emergency evacuation drills at minimum 12 monthly intervals.

Supervisors/Chief Wardens/Work Health and Safety Representatives will:

- Ensure all workers are aware of the Fire and Evacuation Plan (located in “O” Drive under > WHS > Operations > Site Name > Fire & Emergency Preparedness) at site-specific inductions
- Ensure that a copy of the Fire and Evacuation Plan, with current emergency telephone numbers, is kept at each STEPS site
- Ensure that the *Emergency Response Checklist (flipchart)* and Emergency Contact List (i100102) is complete, current and displayed in STEPS workplaces.

Emergency Wardens will:

- Ensure an Evacuation Guidelines and Report (i100101) is completed after each drill or situation and notify the relevant Program Manager, ELT member, Fire Safety Adviser (FSA) and Work Health and Safety Officer (WHSO) of any issues that arise from the evacuation process.

Workers will:

- Ensure they are fully aware of, and understand, the application of the Emergency Response Procedures
- All workers must follow directions of emergency services personnel and emergency wardens.

2.0 DOCUMENTATION

The documents listed below need to be developed and maintained to enable effective responses and recovery to support continued operations following emergencies, events, or incidents. The goal is to provide a safe workplace and to remain operational and deliver services with minimal disruption to workers and customers, participants, and students.

2.1 RISK ASSESSMENT

This is to be completed annually by the Work, Health, and Safety Officer (WHSO) who will contact each Site Manager (including commercial operations and supporting operations) and is to be recorded on the General Risk Assessment Form (i050105).

The purpose of the risk assessment is to identify and assess all the possible events and incidents that could impact the site or business, such as severe weather, flooding, high staff turnover, data attacks, pandemic, work environment issues (such as broken air-conditioning), violence etc.

Part of this process will consider how to distribute information to workers and other stakeholders in the event of an emergency.

Any first responders need to be listed on the risk assessment and reflected in the Emergency Response Checklist (Flipchart) as emergency contacts to enable fast responses if a crisis occurs in a site.

These are to be saved in the “O” Drive under WHS > Operations > Site Name > Fire & Emergency Preparedness folder.

2.2 BUSINESS CONTINUITY PLANS (BCP)

BCPs are to be developed to facilitate business operations or services to be restored as quickly as possible. The number and type of BCPs will be identified in the risk assessment.

Each BCP will be completed with input from the Chief Executive Officer, Executive Manager, Line/Site Manager/Supervisor, and a member of the Human Resources (HR), Information and Communications Technology (ICT), Finance and Marketing and Communications teams.

The BCPs are to be saved in the WHS Folder in “O” Drive.

2.3 FIRE AND EVACUATION PLANS

In consultation with the WHSO and Fire Safety Adviser the following issues must be considered in developing Fire and Evacuation Plans:

- The nature of on-site hazards, e.g., flammable liquids, storage tanks and compressed gases, and measures to be taken in the event of spillages or incidental releases
- The most likely type and scale of an emergency situation or incident
- The most appropriate methods for responding to an incident or emergency situation
- Internal and external communication plans
- The actions required to minimise environmental damage
- Mitigation and response actions to be taken for different types of incident or emergency situation
- The need for a process for post-incident evaluation to establish and implement corrective and preventive actions
- Periodic testing of emergency response procedures
- Training of emergency response workers
- A list of key workers and aid agencies, including contact details (e.g. fire and emergency services, spillage clean-up services)
- Evacuation routes and assembly points

- The potential for an emergency situation(s) or incident(s) at a nearby facility (e.g. plant, road, railway line)
- The possibility of mutual assistance from neighbouring organisations.

These are to be saved in the "O" Drive under WHS > Operations > Site Name > Fire & Emergency Preparedness folder.

3.0 REVIEW

Emergency drills and situations will be reviewed using the Evacuation Guidelines and Report (i100101) after each drill or emergency event. The Fire Safety Adviser will maintain a record of the site schedule for evacuation drills and review each quarter to ensure the drills have been undertaken.

BCPs are to be reviewed annually using the Business Continuity Test and Report Template (i100105). Any changes or updates must be added made to the BCP and the previous BCP needs to be archived in the same folder in "O" Drive.

4.0 DISPLAY

The Emergency Response Checklist (flipchart) and Emergency Contact List (i100102) for the site will be displayed at various locations at each workplace (e.g. lunchrooms, offices).

5.0 COMMUNICATION

All persons in the workplace will be made aware of the content and application of the Emergency Procedures through site specific inductions.

5.1 EMERGENCY RESPONSE TEAM

In the event of an emergency, the following team needs to be assembled and briefed to ensure all responsibilities in response to the emergency or in the BCP are undertaken successfully.

The emergency response team (ERT) will depend on the level and location and scale of the emergency. At a minimum, the ERT must be the Executive Manager, an ELT member, Site/Line Manager and a member of the HR and Marketing and Communications Team.

The ERT will assess the impact of the event/incident to the business and record the following:

1. Damage (e.g. buildings, community, stock)
2. Impact to business (government response, critical functions)
3. Severity of impact (Low, Medium, High e.g. months to rebuild vs 3-day weather event)
4. Action required (repair, replace, relocate for a period)
5. Recovery steps (refer to BCP for guidance)
6. Resources needed (employees, contractors, suppliers etc)
7. Who will action each item identified (assign to an individual) with a due date or an estimated date of completion?

Following the immediate response, it may become necessary to include ICT, Finance, Quality Assurance and Risk, the WHSO and others in the ERT.

Role	Function in the ERT
Executive Manager	Lead and coordinate the disaster/emergency response and recovery. Keep the Chief Executive Officer and/or Managing Director informed of the emergency and the responses. Manage and coordinate additional resources to support operations if needed. Contact other agencies if required (i.e. government, contract managers, first responders, contractors).
Executive Administration Team Member	To collate and record information. Share information as required.
HR Team Member	To coordinate communication with workers for information, updates and worker well-being and welfare. Consider Industrial Relations implications. Brief WHSO to ensure WHS obligations are fulfilled.
Marketing and Communications Team Member	Manage external communications, public relations managed by an external contractor etc.
Others to provide advice or guidance	Finance – insurance, tracking response costs, recording expenditures etc. Quality Assurance & Risk – management of risk, providing documentation and research re contracts, existing tools etc. Others as needed.

6.0 TRAINING

The Fire and Evacuation Plan is to be discussed at least annually at team meetings and reviewed as part of the WH&S Office Inspection Checklist (i060201) or WH&S Nursery Inspection Checklist (i060203) or WH&S Creche Inspection Checklist (i060205).

Emergency Wardens will have yearly refresher training provided by a competent person. Employees who have been appointed as First Aiders will receive training as per the First Aid Procedure (i090400).

7.0 RECORDS MANAGEMENT

Records relating to STEPS workplaces shall be saved in “O” Drive in the WHS folder.

8.0 RELATED DOCUMENTS

Document Name	Document Name
Business Continuity Plan (i100104)	Business Continuity Plan/Review Schedule (i100106)
Business Continuity Test and Report Template (i100105)	Emergency Contact List (i100102)
Evacuation Guidelines and Report (i100101)	*Emergency Response Checklist (flipchart)*
First Aid Procedure (i090400)	Fire and Evacuation Plan (site specific) Located in *'I'* > *Work Health and Safety* > *Site Name* > *Fire & Emergency Preparedness*
General Risk Assessment Form (i050105)	WH&S Office Inspection Checklist (i060201)
WH&S Nursery Inspection Checklist (i060203)	WH&S Creche Inspection Checklist (i060205)

9.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	24 August 2023
Effective Date	28 August 2023	**Document Number**	i100100_v7_230828

(Uncontrolled when printed)

1.6.5 Emergency Response

1.0 RESPONDING TO EMERGENCIES

This procedure provides guidance on planning, documentation and communication of the Emergency Response procedures for all STEPS Group of Companies' (STEPS) workers. This procedure applies to all STEPS workplaces.

1.1 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Provide adequate resources to ensure this procedure is implemented within STEPS.
- Conduct monthly reviews of all incidents and non-conformances.

Site or Program Manager will:

- Ensure that all employees in their area of responsibility are aware of, and understand, the content and application of the Emergency Response procedures for STEPS.
- Ensure that Wardens undertake emergency evacuation drills at minimum 12 monthly intervals.

Supervisors/Chief Wardens/Wardens will:

- Ensure all workers are aware of the Fire and Evacuation Plan (located in *'O'>WHS>Site Name>Fire & Emergency Preparedness>Evacuation Plans>Year i.e. 2023)* at site-specific inductions.
- Ensure that a copy of the Fire and Evacuation Plan, with current emergency telephone numbers, is kept at each STEPS site.
- Ensure that the Emergency Response Checklist (flipchart) and Emergency Contact List (i100102) is complete, current and displayed in STEPS workplaces.

Wardens will:

- Ensure that an Evacuation Guidelines and Report (i100101) is completed after each drill or situation and notify the relevant Site or Program Manager/ELT member and Work Health and Safety Officer (WHSO) of any issues that arise from the evacuation process.
- Attend training and emergency exercises as required.

Workers will:

- Ensure they are fully aware of, and understand, the application of the Emergency Response Procedures and follow directions given by the attending emergency management team and Wardens.

2.0 EMERGENCY RESPONSE PROCEDURES

In the event of a situation arising that may require site evacuation (including a fire, bomb threat, gas leak, natural disaster, chemical spill or any other threatening situation), the person discovering the emergency is to contact the nearest supervisor and advise them of:

- The nature of the emergency.
- The location of the emergency.

The supervisor will notify the Chief Warden/Warden to sound the alarm. Relevant Wardens, Supervisors and Health and Safety Representatives (HSRs) will direct workers to evacuate the workplace.

On receiving an instruction, all workers and visitors are required to leave their work areas and assemble at the emergency assembly point indicated on the emergency evacuation plan.

All workers and visitors are to remain at the assembly area until their name has been checked off as per the In/Out Registers (i100202 or i100203) and are advised it is safe to return to their work area.

On evacuating, the following procedures should be observed:

- Stay calm and encourage others to remain calm and orderly.

- Once evacuation has started, do not go back for valuables or tools.
- If escaping through a smoke filled area, keep low to the ground or floor.
- Feel the surface of closed doors for heat before opening them.
- Do not use lifts or material hoists.
- Close doors to fire escapes behind you.
- If trapped, go to an outer room where the door can be shut and try and attract attention from a window or balcony.
- Proceed to Assembly Area and remain until advised it is safe to return to work.
- Shut down any plant and equipment (if safe to do so).

3.0 INCIDENTS INVOLVING INJURY TO PERSONS

3.1 Minor incidents involving injury to persons

- The person involved in the incident is to report the incident to their supervisor and the appointed First Aider (if applicable).
- The supervisor/First Aider is to either administer first aid, or make a decision as to whether treatment over and above first aid is required and if so, initiate.
- The Reporting Person will record the incident on the WHS Incident Report (i090201) and inform the WHSO.

3.2 MAJOR INCIDENTS INVOLVING INJURY TO PERSONS

Workers present at the incident are to contact 000 or 112 from a mobile phone and provide assistance, notify supervisor/Wardens/other persons within the close vicinity.

The Warden is to:

- In the event of a serious injury, structural damage or environmental spill or leak, ensure the incident scene is not interfered with.
- In the event of a fire or spill, make a decision as to whether the fire and emergency services are required, and if so, provide appropriate notification.
- Order an emergency vehicle.
- Notify the First Aider (if applicable).
- Organise a person, who knows where the incident is, to meet the emergency vehicle at the entrance to the site and act as a guide.
- Notify the WHSO and relevant Site or Program Manager/ELT member.

The supervisor is to record the incident on the WHS Incident Report (i090201) and forward a copy to the WHSO via email at whs@stepsgroup.com.au

3.3 PERSONAL THREAT FROM PARTICIPANTS WITH CHALLENGING BEHAVIOURS

In the event of a personal threat from supporting participants with challenging behaviours please refer to the Managing and De-Escalating Participants Challenging Behaviours Procedure (i051300)

3.4 PERSONAL THREAT FROM CIVIL DISTURBANCE

In the event of a personal threat from civil disturbance, the worker shall:

- Ensure the supervisor is notified immediately of the location and describe situation.
- Initiate action to:
    - Restrict entry to building if possible.
    - Confine or isolate the threat from building occupants.
- Refer to your community emergency plan (remote).
- Report to the supervisor regularly regarding the status disturbance.
- Evacuation should be considered (only if safe to do so).
- Notify the Police by dialling 000 or 112 from a mobile phone and request assistance.
- Inform the WHSO and relevant Program Manager/ELT member as soon as practicable.

4.0 EXTERNAL EMERGENCY

External Emergency includes, but is not limited to, Storms, Cyclone, Floods, Earthquake and Bush Fire.

NOTE: Workers must also refer to their local community Disaster Management Plan and must follow direction given by Emergency Services Personnel.

4.1 STORM/EARTHQUAKE

- Remain in the building and keep well clear of windows
- If in a multi storey building, move to a lower floor
- In all buildings shelter under desks or similar structures that offer protection
- Follow the instructions of Wardens or relevant Emergency Services Personnel
- Turn off or limit the use of mobile phones and encourage others to do the same
- Evacuate the building only if instructed to do so by the Warden or Emergency Services personnel and assist with the evacuation of disabled occupants
- If evacuation is ordered, move to the nominated Assembly Area and do not leave the Assembly Area until advised to do so.

4.2 CYCLONE

Preparation

- Prepare an emergency kit containing:
    - a portable battery radio, torch and spare batteries
    - water containers, dried or canned food and a can opener
    - matches, fuel lamp, portable stove, cooking gear, eating utensils
    - a first aid kit and manual, masking tape for windows and waterproof bags

  - an up to date list of emergency telephone numbers.

- Check with those in the immediate vicinity.

When a ‘cyclone watch’ is issued

- Re-check property for any loose material and tie down (or fill with water) all large, relatively light items such as rubbish bins
- Fill vehicles' fuel tanks
- Check your emergency kit and fill water container.
- Ensure you are aware which is the strongest part of the property you are in
- Tune to your local radio/TV for further information and warnings
- Check with those in the immediate vicinity.

When a ‘cyclone warning’ is issued

Depending on official advice provided by your local authorities as the event evolves; the following actions ‘may’ be warranted.

- Park vehicles under solid shelter (hand brake on and in gear).
- Close shutters or board-up or heavily tape all windows. Draw curtains and lock doors.
- Pack an evacuation kit of warm clothes, essential medications, valuables, important papers, photos and mementos in waterproof bags to be taken with your emergency kit. Large/heavy valuables could be protected in a strong cupboard.
- Remain indoors
- Stay tuned to your local radio/TV for further information.

On warning of ‘local evacuation’

Based on predicted wind speeds and storm surge heights, evacuation may be necessary. Official advice will be given on local radio/TV regarding safe routes and when to move.

- Wear strong shoes (not thongs) and tough clothing for protection.
- Lock doors; turn off power, gas, and water; take your evacuation and emergency kits.
- If evacuating inland (out of town), take pets and leave early to avoid heavy traffic, flooding and wind hazards.
- If evacuating to a public shelter or higher location, follow police and State/Territory Emergency Services directions.
- If going to a public shelter, take bedding needs.

When the cyclone strikes

- Disconnect all electrical appliances. Listen to your battery radio for updates.
- Stay inside and shelter (well clear of windows) in the strongest part of the building, i.e. cellar, internal hallway or bathroom.
- Keep evacuation and emergency kits with you.

- If the building starts to break up, protect yourself with mattresses, rugs or blankets under a strong table or bench or hold onto a solid fixture, e.g. a water pipe.
- Beware the calm 'eye'. If the wind drops, don't assume the cyclone is over; violent winds will soon resume from another direction. Wait for the official 'all clear'.
- If driving, stop (handbrake on and in gear) - but well away from the sea and clear of trees, power lines and streams. Stay in the vehicle.

After the cyclone

- Don't go outside until officially advised it is safe.
- Check for gas leaks. Don't use electric appliances if wet.
- Listen to local radio for official warnings and advice.
- If you have to evacuate, or did so earlier, don't return until advised. Use a recommended route and don't rush.
- Beware of damaged power lines, bridges, buildings, trees and don't enter flood waters.
- Heed all warnings and don't go sightseeing. Check/help neighbours instead.
- Don't make unnecessary telephone calls.

4.3 FLOOD

- Remain in the building and keep well clear of building access points;
- Follow the instructions of relevant Emergency Services personnel;
- Switch off any electrical equipment and gas that could be affected by water.
- Move any chemicals, documents, equipment and valuables to a safe area if time permits.
- Evacuate the building only if instructed to do so by Emergency Services personnel and assist with the evacuation of disabled occupants;

4.4 BUSH FIRE

- Close all windows and external doors
- Remain, or go inside and await further instructions from Emergency Services personnel.
- Do not evacuate from the site or drive vehicles until or unless directed to do so by the Warden or Emergency Services Personnel.

It is recommended that you are aware of your local community emergency broadcasting service (e.g. ABC local station) which will provide you with updates and advice.

5.0 DANGEROUS GOODS/HAZARDOUS MATERIALS

On discovering a dangerous goods/hazardous materials spill, workers should contact their supervisor advising the following:

- location of the spill
- size of spill

- type of spill (i.e. what has been spilt).

If the spill gives off toxic or noxious fumes the Warden/supervisor will:

- Turn off air conditioning and recirculation fans – ventilate to the open air if possible
- If threat to life exists, evacuate as per the emergency evacuation procedure.

If the spill is a suspected flammable material:

- Remove any ignition sources (only if safe to do so)
- Evacuate all persons in immediate danger
- Notify Emergency Services by dialling 000 or 112 from a mobile phone and request assistance
- Do not attempt to re-enter the affected area
- Remain at the Assembly Area until advised by Emergency Services
- Notify the WHSO and relevant Site or Program Manager/ELT member.

6.0 GAS LEAKAGE

On discovering a gas leak, workers should contact their supervisor advising the following:

- location of the leak
- size of leak.

The supervisor will notify all workers at the worksite advising of the type and extent of the emergency and contact Emergency Services and:

- Isolate the gas supply at the source (if safe to do so)
- Shut down the air conditioning to prevent the spread of any flammable and/or toxic gases
- Remove all ignition sources (if safe to do so). Turn off the electrical supply
- Evacuate all persons in immediate danger as per emergency evacuation procedure
- Notify Emergency Services by dialling 000 or 112 from a mobile phone and request assistance
- Remain at the Assembly Area until further advised by Emergency Services
- Notify the WHSO and relevant Site or Program Manager/ELT member.

7.0 MOBILE PLANT INCIDENT

In the event of a mobile plant incident, the supervisor/Warden should:

- Alert all persons nearby and if required provide assistance
- Assist any person in immediate danger (only if safe to do so)
- Control the movement of workers around the area
- Notify Emergency Services by dialling 000 or 112 from a mobile phone and request assistance

- DO NOT move the plant if a person has been injured unless it is required for safety reasons.

8.0 STRUCTURAL COLLAPSE

In the event of Structural Collapse, the supervisor/Warden should:

- Alert all persons nearby and request assistance
- Assist any person in immediate danger and evacuate (only if safe to do so)
- If required, notify Emergency Services by dialling 111 or 112 from a mobile phone and request assistance.
- Maintain control of persons at the Assembly Area
- Notify the WHSO and relevant Program manager/ELT member.

9.0 ELECTRICAL INCIDENT – PLANT HITTING OR WORKER TOUCHING LIVE POWER SUPPLY

ISOLATE THE POWER AT THE RELEVANT SWITCHBOARD IF ON SITE

In the event of an electrical incident the supervisor/Warden will:

- Alert all persons nearby and request assistance from Emergency Services by dialling 000 or 112 from a mobile phone.
- If power lines are involved contact the relevant electricity entity immediately
- Assist any person in immediate danger (only if safe to do so)
- Control the movement of workers around the area
- DO NOT move the plant if involved until advised safe to do so by emergency services
- Notify the WHSO or relevant Site or Program Manager/ELT member.

NOTE: A licensed electrician must inspect any identified electrical equipment involved in an incident and give the Supervisor/WHSO a certificate of safety as soon as practicable after any electrical incident. The equipment must not be used until the safety certificate has been issued.

10.0 BOMB THREATS

10.1 TELEPHONE BOMB THREAT

Action to be taken by recipient:

DO NOT HANG UP THE PHONE

- Complete Bomb Threat Checklist (i100201) with as much detail as possible. Try to keep the caller talking to gain more information.
- Notify your supervisor who will notify the Police (000 or 112 from a mobile phone) and Warden/s but do not do or say anything that may encourage irrational behaviour.
- The supervisor and the Chief Warden/Warden will take further action as required and notify the WHSO and relevant Program Manager/ELT member.

- Action to be taken by Wardens as directed by Police.

10.2 IF A SUSPECTED EXPLOSIVE DEVICE IS FOUND

- DO NOT touch, cover or move the item.
- Clear the area of all occupants and, if able, isolate the area preventing all persons from entering the area.
- Notify a supervisor/Warden immediately who will take further action as required and notify the WHSO and relevant Program Manager/ELT member.
- Follow the directions given by the supervisor/Warden/Police.

11.0 TRAINING

Workers will be informed of this procedure during their site specific Induction and this procedure is to be discussed at least annually at Team Meetings in conjunction with the Fire and Evacuation Plan and Emergency Planning Procedure (i100100).

12.0 RELATED DOCUMENTS

Document Name	Document Name
Bomb Threat Checklist (i100201)	In/Out Register - Employees (i100202)
In/Out Register - Visitors/Contractors (i100203)	Emergency Planning Procedure (i100100)
Evacuation Guidelines and Report (i100101)	Emergency Contact List (i100102)
Managing and De-Escalating Participants Challenging Behaviours Procedure (i051300)	WHS Incident Report (i090201)
Fire and Evacuation Plan (located in *'O'>WHS>Site Name>Fire & Emergency Preparedness>Evacuation Plans>Year i.e. 2023*	Emergency Response Checklist (flipchart)

13.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	29 February 2024
Effective Date	7 March 2024	**Document Number**	i100200_v7_240307

(Uncontrolled when printed)

1.6.6 First Aid

1.0 PROVIDING FIRST AID

This procedure outlines the requirements for STEPS to provide immediate and effective first aid to workers or others in the workplace and includes the:

- Planning for First Aid.
- Provision of adequate First Aid facilities.
- Provision of adequate number of First Aiders.
- Provision of appropriately trained First Aiders.

2.0 DEFINITION OF FIRST AID

First Aid	Is the immediate treatment or care given to a person suffering from an injury or illness until more advanced care is provided or the person recovers
First Aider	Is a person who has successfully completed a nationally accredited training course or an equivalent level of training that has given them the competencies required to administer first aid.
Appointed First Aider	The Executive Manager of the region/area nominates an employee to administer first aid in the workplace and this information is included on a workplace notice displayed in the relevant workplace.

3.0 RESPONSIBILITIES AND ACCOUNTABILITIES

Executive Leadership Team will:

- Ensure that sufficient resources are allocated to fully implement this procedure.
- Ensure appropriately qualified First Aiders are appointed (if applicable).

Supervisors will:

- Ensure that any worker under their care or in their workplace is aware of:
  - This procedure and encouraging compliance.
  - How to use any first aid or safety equipment correctly.
  - Notification and reporting procedures.
- Ensure appropriate first aid equipment is available in the workplace.
- Ensure first aid equipment in the workplace is appropriate for the identified hazards and associated risks.

- Ensure that, as part of the site orientation and Work Health and Safety (WHS) Induction, all workers are made aware of who the appointed First Aiders are and how to contact them (if applicable).
- Ensure that requests for restocking first aid kits are processed promptly.
- Clear signage is prominently displayed in and around their area of responsibility.

Employees will:

- Be aware of the emergency contact information for their worksite.
- Be aware of the name, contact number and work location of their appointed First Aider (if applicable).
- Be aware of the location of the first aid kit and Automated External Defibrillator (AED) (if applicable).

4.0 PLANNING FOR FIRST AID

The planning of first aid is not a control measure which prevents or minimises work injury or work caused illness but is actually a control measure to deal with injury or illness that has already occurred. In relation to the provision of first aid, a modified version of the risk management process can also be used to decide on appropriate first aid equipment, facilities and number of First Aiders.

The following steps can be used to plan appropriate first aid coverage within sites:

- Identify the hazards that may cause injury or illness using General Risk Assessment.
- Assess the risk, type and extent of work injuries and work caused illnesses that may occur.
- Decide on appropriate first aid equipment, facilities, services (including trained employees) which can best address the injuries or illnesses likely to occur and which are suitable considering:
    - The size.
    - Layout.
    - Location of the workplace. For example, a workplace with a large physical area may require that first aid be made available in more than one location a workplace which is some distance from medical facilities and/or has access problems such as poor road quality or a proneness to flooding may require employees with advanced first aid training.
- Implement the chosen first aid equipment, facilities and services to effectively manage the injuries and illnesses.
- Monitor and review first aid equipment, facilities and services to ensure they continue to meet requirements.
- Decide on the qualifications of the First Aider/s based on the risk assessment outcomes.

5.0 FIRST AID TREATMENT – RECORDING AND RECORD MAINTENANCE

All treatment given by a First Aider must be recorded in the WHS Incident Report.

The following process chart highlights the actions to be taken in each instance of an incident.

6.0 FIRST AID RECORDING REQUIREMENTS

Insignificant and Minor Injury/Illness	Treated by employee/currently trained First Aider with treatment provided
Moderate Injury/Illness	Treated by employee/currently trained First Aider and referral for treatment or medical attention as required
Major or Catastrophic Serious bodily injury or Illness	Contact Emergency Services, for guidance and where required convey injured party to local Medical Centre or Hospital. Notify WHS Officer (WHSO)/Executive Manager – Human Resources.

7.0 FIRST AID KIT CONTENTS

First aid kits will be maintained and re-stocked by supervisors or nominated persons and/or first aider (if applicable).

First aid kits must be compiled after a risk assessment has been performed to ensure that its contents are adequate for the type of work being performed. The minimum items required to be included in the First Aid Kit are detailed in the First Aid Kit Content List, the list is laminated and secured inside the Kit. Further details are specified in the relevant regulations and *First Aid in the workplace Code of Practice 2021*.

Medication, including analgesics such as paracetamol and aspirin, should not be included in first aid kits because of their potential to cause adverse health effects in some people including asthmatics, pregnant women and people with medical conditions. The supply of these medications may also be controlled by drugs and poisons laws. Workers requiring prescribed and over-the-counter medications should carry their own medication for their personal use as necessary.

8.0 FIRST AID KIT LOCATIONS

Each kit should be located close to running water, if possible, and in a readily accessible place (kitchens or staff lunchrooms may be appropriate locations).

The location of first aid kits should be signposted with the appropriate safety sign (a white cross on green background) and displayed in the immediate vicinity.

9.0 FIRST AIDER NUMBERS AND TRAINING

It is necessary in every workplace to determine the number of nominated First Aider/s to ensure adequate coverage through risk assessment. Consideration is required of:

- The size of the workplace and the number of workers.
- Shift arrangements in place.
- Leave and other absence coverage.

All First Aid Training must be provided by any appropriately authorised training provider and the course must be certified. Upon completion of the training, a copy of the Certificate of Competency must be verified by the Supervisor, recorded in the Human Resources Information System (HRIS) and saved on the employee's personnel file. The minimum level of training required is HLTAID011 Provide First Aid, provide CPR and provide basic emergency life support.

Note that while first aid competencies are to be re-certified every three years, cardiopulmonary rescue (CPR) re-certification is required to be undertaken every 12 months.

10.0 HAZARDOUS SUBSTANCES

Hazardous chemicals Safety Data Sheets (SDS) must be available and accessible to the First Aider where an injury or illness has involved, or potentially involved, the use of such a substance. The SDS should also be provided in any referral to seek further medical attention and must be transported with the injured person. Electronic copies are available in O: drive>WHS>Operations>Site Location>SDS.

11.0 RELATED DOCUMENTS

Document Name	Document Name
General Risk Assessment (i050105)	WHS Incident Report (i090201)
First Aid Kit Contents List (i090403)	

IMS_i090400_FirsAid_v3_240923_7834

1.6.7 Hazardous Manual Tasks

1.0 INTRODUCTION

STEPS Group Australia (STEPS) recognises that musculoskeletal injuries and disease, whether occurring suddenly or over time may have a significant impact and can be linked to manual handling practices. Accordingly STEPS has adopted procedures to eliminate or minimise manual handling at all its workplaces.

Most jobs involve carrying out some type of manual task using the body to move or hold an object, people or animals. Manual tasks cover a wide range of activities such as moving boxes, stacking shelves, and entering data into a computer.

1.1 RESPONSIBILITIES AND ACCOUNTABILITIES

Executive Leadership Team will:

- Ensure that sufficient resources are allocated to fully implement this procedure.
- Schedule and conduct manual handling training, or liaise with WHS to engage a competent manual handling Trainer to conduct training as required.

Senior Leadership Team will:

- Ensure that workers and the Work Health and Safety Officer (WHSO) are consulted in regard to the manual handling hazards and the development of control measures.

Supervisors will ensure:

- Manual handling hazards are identified.
- Risk assessments are completed on all manual tasks.
- All workers under their control are appropriately skilled and trained in safe manual tasks when working within the workplace.
- Ensure new workers receive an appropriate induction and are competent to undertake manual tasks prior to working without direct supervision.
- Ensure all workers understand and adhere to safe work procedures.

WHSO and Health and Safety Representatives (HSR's) will:

- Ensure positive action is taken immediately to stop any unsafe act observed.
- Take immediate positive, preventative and corrective action in line with the hazard reporting process, for any safety concern identified in the workplace.

Workers will:

- Not place themselves or others at risk of injury.
- Report hazards associated with manual handling and consult with supervisors in relation to appropriate control measures.

2.0 WHAT IS A MUSCULOSKELETAL DISORDER (MSD)?

A musculoskeletal disorder, as defined in the WHS Regulations, means an injury to, or a disease of, the musculoskeletal system, whether occurring suddenly or over time. It does not include an injury caused by crushing, entrapment (such as fractures and dislocations) or cutting resulting from the mechanical operation of plant.

MSDs may include conditions such as:

- sprains and strains of muscles, ligaments and tendons

- back injuries, including damage to the muscles, tendons, ligaments, spinal discs, nerves, joints and bones
- joint and bone injuries or degeneration, including injuries to the shoulder, elbow, wrist, hip, knee, ankle, hands and feet
- nerve injuries or compression (e.g. carpal tunnel syndrome)
- muscular and vascular disorders as a result of hand-arm vibration
- soft tissue hernias
- Chronic pain.

MSDs occur in two ways:

- gradual wear and tear to joints, ligaments, muscles and inter-vertebral discs caused by repeated or continuous use of the same body parts, including static body positions
- sudden damage caused by strenuous activity, or unexpected movements such as when loads being handled move or change position suddenly

Injuries can also occur due to a combination of these mechanisms, for example, body tissue that has been weakened by cumulative damage may be vulnerable to sudden injury by lower forces.

3.0 WHAT IS A HAZARDOUS MANUAL TASK?

A hazardous manual task, as defined in the WHS Regulations, means a task that requires a person to lift, lower, push, pull, carry or otherwise move, hold or restrain any person, animal or thing involving one or more of the following:

- repetitive or sustained force
- high or sudden force
- repetitive movement
- sustained or awkward posture
- exposure to vibration

These factors (known as characteristics of a hazardous manual task) directly stress the body and can lead to injury.

4.0 IDENTIFYING HAZARDOUS MANUAL TASKS

The first step in managing risks from carrying out manual tasks is to identify those tasks that have the potential to cause MSDs. The Manual Task Checklist (i050401) can be used to identify the level of risk associated with the manual task.

Hazards that arise from manual tasks generally involve interaction between a worker and:

- the work tasks and how they are performed
- the tools, equipment and objects handled
- the physical work environment

The Supervisor is to complete the Manual Task Checklist (i050401) with the worker where risks from hazardous manual tasks have been identified.

5.0 THE RISK MANAGEMENT PROCESS FOR MANUAL TASKS

After the Manual Task Checklist (i050401) has been completed the information is to be transferred onto the Manual Task Risk Assessment (i050402) which will document the measures used to eliminate or control the risks where the risk is determined as moderate to catastrophic.

This process involves the following steps:

1. Identify

What is the manual task?

Using the body to lift, lower, push, pull, carry or otherwise move, hold or restrain any person, animal or thing.

Is the manual task hazardous?

- Application of force:
  - Repetitive
  - Sustained
  - High
  - Sudden
- Posture:
  - Sustained
  - Awkward
- Movement:
  - Repetitive
- Exposure to vibration

2. Assess

What is the risk of MSD?

- How often and how long are specific postures, movement or forces performed or held?
- What is the duration of the task?
- Does the task involve high or sudden force?
- Does the task involve vibration?

What is the source of risk?

- Work area design and layout
- Systems of work
- Nature, size, weight and number of persons, animals or things handled
- Work environment

3. Control

Is the task necessary?

Can the source of risk (work area layout, environment, etc.) be changed?

Can mechanical aids be used to perform the task?

What training is needed to support the control measures?

4. Review

When to review:

- when the control measure is no longer effective
- before a change at the workplace that is likely to give rise to a new or different health and safety risk that the control measure may not be effectively control
- if a new hazard or risk is identified
- if a health and safety representative at the workplace requests a review

Note: Further information can be obtained from Safe Work Australia 'Hazardous manual tasks. Code of Practice 2011'

Submit the completed Manual Task Checklist (i050401) and Manual Task Risk Assessment (i050402) to the Supervisor for further action as required. A copy of the Manual Task Checklist (i050401) and Manual Task Risk Assessment (i050402) is to be submitted to the WHSO for recording and reporting purposes.

6.0 ERGONOMICS

Prolonged periods of sitting can place heavy demands on our posture and increase your risk of a range of potentially serious health problems, even if you engage in regular exercise.

If you sit at your desk in an awkward position or for a long period, you may suffer pain, discomfort or an injury.

Typical injuries include sprains and strains of the neck, back, shoulders, wrists or hands. In order to minimise these risks, it is important to have a good workstation design, layout and setup as well as having a variety of tasks and opportunities to move around throughout the day.

A Workstation Ergonomics Checklist is available from the HSR's or WHSO upon request and can be used to determine if there are risks present to the worker.

Further information about setting up computer workstations can be found in the Ergonomic Guide to Computer Based Workstations and various office/static stretches, and fact sheets which are available on the STEPS Intranet (WHS Tab).

7.0 TRAINING

STEPS will provide appropriate education to workers on this procedure as part of the WHS Induction. Employees identified in high-risk areas (e.g. Community Services, Nursery) will receive Manual Handling training upon commencement and on a regular basis thereafter.

Job specific training will be given to workers, particularly on how their work could be completed with the minimal amount of risk. This training will include relevant Job Safety Environmental Analyses (JSEA) and General Risk Assessments.

8.0 RELATED DOCUMENTS

Document Name	Document Name
Manual Task Checklist (i050401)	Manual Task Risk Assessment (i050402)
Safe Work Australia ‘Hazardous manual tasks. Code of Practice 2011 *Refer to* Safe Work Australia	Ergonomic Guide to Computer Based Workstations - *Workplace Health & Safety Qld, 2012* This document and further information can be found on the *'STEPS Intranet > WHS > Office Ergonomics and Info'* tab
Workstation Ergonomics Checklist *Refer to WHSO for a copy*	

9.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	17 October 2023
Effective Date	3 November 2023	**Document Number**	i050400_v3_231103

(Uncontrolled when printed)

1.6.8 Hazardous Substances Management

1.0 PURPOSE

This procedure outlines the management of all hazardous and non-hazardous substances including Dangerous Goods for STEPS Group Australia (STEPS).

1.1 DEFINITIONS

Hazardous Substance	Any substance, which has the potential to cause harm. That is any substance which is: • Listed by the Australian Safety Compensation Council (ASCC) on the Designated Hazardous Substances List, or Determined hazardous by the manufacturer or supplier on the basis of the ASCC approved criteria for the classification of hazardous substances.
Dangerous Good	Goods which have been classified as dangerous goods, or contain substances which have been classified as dangerous goods.
Safety Data Sheets (SDS)	Information sheets that provide technical information in relation to substances. **NOTE:** a product Data Sheet is not a Safety Data Sheet.

Biological monitoring	a) The measurement and evaluation of a substance, or its metabolites, in the body tissue, fluids or exhaled air of a person exposed to the substance; or b) Blood lead level monitoring. Blood lead level means the concentration of lead in whole blood expressed in micromoles per litre (µmol/L) or micrograms per decilitre (µg/dL). Blood lead level monitoring means the testing of the venous or capillary blood of a person by a laboratory accredited by NATA, under the supervision of a registered medical practitioner to determine the blood lead level.
National exposure standard	Means the exposure standard for hazardous chemicals in the Adopted National Exposure Standards for Atmospheric Contaminants in the Occupational Environment
Relevant period	Means the exposure period stated in former NWHSC document entitled ‘Exposure Standards for Atmospheric Contaminants in the Occupational Environment’.
Registered medical practitioner	Means a person registered under the Health Practitioner section National Law to practise in the medical profession (other than as a student).
Airborne contaminant	Means a contaminant in the form of a fume, mist, gas, vapour or dust, and includes microorganisms.
Asbestos	Means the asbestiform varieties of mineral silicates belonging to the serpentine or amphibole groups of rock forming minerals including the following: actinolite asbestos, grunerite (or amosite) asbestos (brown), anthophyllite asbestos, chrysotile asbestos (white), crocidolite asbestos (blue), tremolite asbestos, and a mixture that is a combination of 1 or more of these minerals.
Asbestos containing material (ACM)	Means any material or thing that as part of its design contains asbestos. Asbestos-contaminated dust or debris (ACD) means dust or debris that has settled within a workplace and is, or is assumed to be, contaminated with asbestos.
In situ asbestos	Asbestos or ACM installed in a structure or plant, but does not include naturally occurring asbestos.
Respirable asbestos fibre	Means an asbestos fibre that: a) is less than 3 micrometres wide; b) more than 5 micrometres long; and c) has a length to width ratio of more than 3:1.
Chemical identity	A name, in accordance with the nomenclature systems of the International Union of Pure and Applied Chemistry or Chemical Abstracts Service or a technical name that gives a chemical a unique identity.
Contaminant	Means any substance that may be harmful to health or safety.
Exposure standard	Other than in part 4.1 and sections 367B and 367D of WHS Regulations 2011, means an exposure standard in the Workplace Exposure Standard for Airborne Contaminants.

Hazchem Code	Means a Hazchem Code under the ADG Code, also known as an Emergency Action Code.
Health monitoring	Of a person, means monitoring the person to identify changes in the person's health status because of exposure to particular substances.
Membrane filter method	Means the membrane filter method described in the Guidance Note on the Membrane Filter Method for Estimating Airborne Asbestos Fibres [NWHSC: 3003 (2005)].

2.0 HAZARDOUS SUBSTANCE REGISTER

All hazardous substances used and stored must be identified on the SDS Master Register (i050501 - *Refer to the WHS Officer*).

2.1 SAFETY DATA SHEETS (SDS)

All Safety Data Sheets (SDS) must:

- Be available to workers who are required to use the substance;
- Identify that the substance is a designated hazardous substance;
- Be readily accessible and easily understood by those required to use them;
- Be updated at least every 5 years;
- Be written in English; and
- State an Australian address for SDS emergency contact details.

All contracts undertaken for the supply of hazardous substances must include provision for the supply of an appropriate SDS and include notification of any updates or changes.

A copy of current SDS shall be maintained for all substances considered hazardous and will form part of the SDS Master Register (i050501) located in O Drive.

All sites must have a folder containing copies of current SDS and a completed SDS Product Register (tab 2 of the SDS Master Register – i050501) ensuring the folder is located within easy access to the hazardous substances.

The Supervisor will:

Ensure all workers are aware of the folder location and the use of SDS;

- Contact WHS and arrange for the SDS details to be added to the SDS Master Register (i050501) and be accessible to workers;
- Arrange for a risk assessment to be conducted on the way that the substance will be used;
- Arrange for personal protective equipment (PPE) to be purchased and stored at the locations where the substance will be used;
- Arrange for training of workers in the safe use of the substance;
- Review the use, storage and PPE for the substance during inspections of work areas; and
- Ensure housekeeping is maintained to high standards in areas where substances are stored.
- Ensure that all SDSs are dated within the past 5 years.

Where a substance is also a Dangerous Good, the WHS Officer will ensure:

Environmental and storage requirements stipulated in the SDS are complied with;

- Signage is installed at storage locations for the substance;
- Signage must be in accordance with the relevant Work Health and Safety Regulations and AS1319 Signage for the Occupational Environment; and
- Spill kits must be stored in the area where the substance will be stored, decanted and used.

3.0 RISK ASSESSMENT

Prior to purchasing, or beginning to use any hazardous substance, a risk assessment must be undertaken to assess the risks involved with the handling of that substance. A record of the date of the risk assessment will be recorded on SDS Master Register (i050501).

Risk Assessments must be undertaken using the guidelines contained in the Hazardous Chemicals Code of Practice (refer to the WHS Officer for further information). The Risk Assessment must consider all sources of information and in particular:

- Information from the applicable SDS;
- The type and quantity of the hazardous substance to be used;
- The storage, handling and disposal requirements for the substance;
- The need for personal or environmental monitoring;
- The need for medical surveillance; and
- Personal and environmental surveillance must be undertaken by appropriately qualified persons.

4.0 RISK CONTROL

Measures to eliminate or reduce risk shall be developed in line with the Risk Management Procedure (i050100) and a Risk Assessment conducted using the Hazardous Substance & Dangerous Goods Risk Assessment (i050502).

Control measures chosen shall be documented in accordance with the products SDS. This risk assessment must be kept for seven years. Risk assessments for hazardous substances that contain toxic substances as listed in the Work Health and Safety Act 2011 (Qld) or relevant State/Territory legislation will be kept for 30 years.

5.0 DISPOSAL

All hazardous substances no longer required shall be disposed of in accordance with the provision outlined in the SDS.

6.0 EMERGENCY RESPONSE

Any emergency situation arising from storage or use of hazardous substances shall be addressed through the Emergency Response Procedure (i100200).

The SDS Master Register (i050501) must be readily available for the Emergency Services.

7.0 CONTRACTORS

All hazardous substances which may be required to be used by contractors shall be identified and the relevant supervisor shall ensure that full risk assessments have been undertaken and received.

Each contractor supplying services to STEPS will be required to provide the necessary SDS and all related personal protective equipment, safety equipment and instructions for the job being undertaken.

8.0 TRAINING

Records of training and induction on hazardous substances will be kept for 5 years stating the date of the session, the topics dealt with, the name of the person who conducted the session, and the names of the workers who attended. Training records for toxic substances will be kept for 30 years.

All workers required to work with potentially hazardous substances will be properly trained in their use and be aware of the potential risks. Additional training in the use of SDS shall also be provided as part of the Induction Program.

9.0 RECORD MAINTENANCE AND REVIEW

All SDS and the SDS Master Register (i050501) shall be reviewed at least every 3 months.

10.0 RELATED DOCUMENTS

Document Name	Document Name
SDS Master Register (i050501) *Refer to the WHS Officer for further information*	Hazardous Substance & Dangerous Goods Risk Assessment (i050502)
Risk Management Procedure (i050100)	Emergency Response Procedure (i100200)
Managing Risks of Hazardous Chemicals in the Workplace Code of Practice 2021 (R*efer to the WHS Officer for further information)*	Work Health and Safety Act 2011 or other relevant state/territory legislation

11.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	23 May 2024
Effective Date	27 May 2024	**Document Number**	i050500_v5_240527

(Uncontrolled when printed)

1.6.9 Incident Notification

1.0 NOTIFYING INCIDENTS TO RELEVANT PARTIES

The purpose of this procedure is to provide a method for the reporting and recording of all incidents, serious illnesses, illnesses and dangerous incidents that occur in STEPS Group of Companies (STEPS) workplaces, including the steps to be taken where incidents are required to be notified to the Statutory Body.

1.1 DEFINITIONS

Notifiable Incidents as defined in the WHS Act are:	a) the death of a person b) a serious injury or illness of a person c) a dangerous incident.
Serious injury or illness of a person means an injury or illness requiring the person to have-	a) Immediate treatment as an in-patient in a hospital b) Immediate treatment for: i. the amputation of any part of his or her body ii. a serious head injury iii. a serious eye injury iv. a serious burn v. the separation of his or her skin from an underlying tissue (for example, de-gloving or scalping) vi. a spinal injury vii. the loss of a bodily function viii. serious lacerations. c) Medical treatment within 48 hours of exposure to a substance; and includes any other injury or illness prescribed under a regulation but does not include an illness or injury of a prescribed kind.
A dangerous incident means an incident in relation to a workplace that exposes a worker or any other person to a serious risk to a person's health or safety emanating from an immediate or imminent exposure to-	a) an uncontrolled escape, spillage or leakage of a substance b) an uncontrolled implosion, explosion or fire c) An uncontrolled escape of gas or steam d) An uncontrolled escape of a pressurised substance e) Electric shock

	f) The fall or release from a height of any plant, substance or thing g) The collapse, overturning, failure or malfunction of, or damage to, any plant that is required to be authorised for use under a regulation h) The collapse or partial collapse of a structure i) The collapse or failure of an excavation or of any shoring supporting an excavation j) The inrush of water, mud or gas in workings, in an underground excavation or tunnel h) The interruption of the main system of ventilation in an underground excavation or tunnel i) Any other event prescribed under a regulation; but does not include an incident of a prescribed kind.
Serious electrical incident	Is an incident involving electrical equipment if, in the incident, a person:- • is killed by electricity • receives a shock or injury from electricity, and is treated for the shock or injury by or under the supervision of a doctor • receives a shock or injury from electricity at high voltage, whether or not the person is treated for the shock or injury by or under the supervision of a doctor.
Dangerous electrical event	Includes: • When a person, for any reason, is electrically unsafe around high voltage electrical equipment, even if the person doesn't receive an electric shock or injury • Significant property damage caused by electricity or something originating from electricity e.g. electrical fire • Unlicensed electrical work • Unsafe electrical work • Unsafe electrical equipment or electrical equipment that does not have electrical equipment safety system (EESS) approval markings.

2.0 INCIDENT REPORTING AND NOTIFICATION

It is the responsibility of all workers to report incidents. All incidents including near misses occurring in the workplace shall be reported immediately to the supervisor. The WHS Incident Report (i090201) form is to be used to report, record and investigate all workplace incidents.

Supervisors are responsible for:

- Notifying the Work Health and Safety (WHS) Officer/Executive Manager – HR that an incident has occurred
- Assisting the injured worker to complete the WHS Incident Report (i090201) form
- Ensuring all workplace incidents are recorded in the approved form as soon as practicable but within a maximum of twenty four hours of becoming aware of the incident.

All incidents are to be reported using the following escalation methodology and retained for a period of not less than seven years.

3.0 MANAGEMENT REPORTING PROCESS

Incident Type	Reporting (phone/in person)	Managers Notified	Escalation Timeline	Notification Process and Response
Death	Supervisor, CEO AND Managing Director	WHS Officer AND Executive Manager - HR	Immediately	Supervisor/WHS Officer to attend site immediately and take control of notification to authority. WHS Officer is to notify the Executive Manager - HR, CEO and Managing Director and keep management informed of the incident and outcomes from investigation and regulatory body or other inspections.
Serious Injury & Illness	Supervisor, WHS Officer	Executive Manager - HR, CEO and Managing Director	Immediately	Supervisor/WHSO Officer will attend site and review incident and report to Executive Manager - HR on progress of investigation and corrective actions and outcomes.
Dangerous Event & Environmental Incidents	Supervisor, WHS Officer	Executive Manager - HR, CEO Managing Director	Immediately	Supervisor/WHS Officer to attend site immediately and take control of notification to authority. Keep Executive Manager - HR, CEO and Managing Director informed of the incident and outcomes from investigation and regulatory body or other inspections.

4.0 MANAGING INCIDENTS INVOLVING DEATH, GRIEVOUS BODILY HARM OR DANGEROUS EVENTS

- Written notification must be submitted within 48 hours if requested by the regulator
- The incident site is preserved until an inspector arrives or directs otherwise. However, this doesn't prevent any action to help an injured person or make the site safe.

The notice must be given by the fastest possible means - which could be by telephone or in writing, for example by email or on-line.

All incidents involving death, serious bodily injury or a dangerous event are to be reported to the appropriate Statutory Body by telephone immediately and subsequently on the WHS Incident Report (i090201) form and Statutory Body forms and retained for a period of not less than five years.

Where an incident results in the death of a person, the WHS Officer/Executive Manager HR are to notify the applicable Statutory Body and the CEO and Managing Director by phone and in writing, after becoming aware of the death.

Serious incidents involving medical treatment or admission to a hospital must be immediately reported to the WHS Officer/Executive Manager - HR who will notify the relevant Statutory Body. The person directly involved in the incident, (i.e. the injured person) in conjunction with the relevant supervisor and WHS Officer shall raise an incident report and commence an investigation of the incident.

5.0 RELATED DOCUMENTS

Document Name	Document Name
WHS Incident Report (i090201)	

6.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	24 August 2023
Effective Date	28 August 2023	**Document Number**	i090200_v4_230828

(uncontrolled when printed)

1.6.10 Infection Prevention

1.0 GENERAL

Effective infection control is central to providing high quality services to participants and a safe working environment for STEPS Group of Companies (STEPS) workers and any others who may come into the workplace.

STEPS will manage the risk to participants and workers contracting an infectious and/or preventable disease by identifying infection risks related to the organisation and implementing precautions that are proportionate to those risks.

As a registered NDIS Provider, STEPS complies with:

- The NDIS Practice Standards and Quality Indicators (Nov 2021)
- Relevant State, Territory and Federal Government requirements.

1.0 VACCINATIONS

Whilst most vaccinations are not a mandatory requirement, it is recommended that medical advice be sought about appropriate vaccination measures for the following preventable diseases:

- Influenza
- COVID-19
- Hepatitis A and B
- Measles, Mumps and Rubella (MMR)
- Varicella (Chicken Pox)
- Diphtheria, Tetanus and Pertussis (DTP – commonly known as the ‘whooping cough’ injection)
- Q Fever.

2.0 INFECTION PREVENTION

Stopping the spread of infection is everyone’s responsibility and includes:

- Practicing good hand hygiene
- Following respiratory hygiene/cough etiquette
- Wearing Personal Protective Equipment (PPE) where required or as directed
- Correctly handling medical utensils
- Correctly cleaning work environments.

3.1 HAND HYGIENE

Good hand hygiene must be performed:

- Before and after eating
- Before and after touching a participant
- After exposure to bodily fluids or substances
- After the removal of gloves
- After coughing or sneezing
- After going to the toilet
- When changing tasks and after touching potentially contaminated surfaces.

Good hand hygiene may be performed by using soap and water or an alcohol-based hand sanitiser. Soap and water should always be used if the hands are visibly soiled.

Wash hands regularly with soap and water for at least 20 seconds and dry them completely, preferably with clean, single-use paper towels. If using an alcohol-based hand sanitiser it is recommended that the alcohol-based hand rub contain 60% ethanol or 70% isopropanol as the active ingredient. The use of hand sanitiser should be supported by the following:

- A diagram demonstrating the correct procedure for using alcohol-based hand rub
- Alcohol-based hand rub must be stored, and used, away from heat and naked flames
- No tasks should be attempted until hands are completely dry.

Workers that have cuts, sores or abrasions on their hands must exercise extra caution by covering with a waterproof dressing and wearing gloves where required.

The use of gloves is not an alternative to hand hygiene.

3.2 PERSONAL HYGIENE

Workers must always adhere to standard personal hygiene practices when on shift with STEPS.

Standard personal hygiene requirements include but are not limited to:

- Good hand hygiene
- Keeping hair clean and pulled back from your face
- Wearing minimal or no jewellery
- Wear clean clothing
- Practicing regular and proper hand washing techniques
- Keeping fingernails short and clean
- Wash body, hair (including facial hair) and clothes thoroughly every day
- Avoid touching your face, eyes, nose and mouth
- Have no unnecessary and intentional physical contact, for example, hugging and patting backs.

3.3 RESPIRATORY HYGIENE/COUGH ETIQUETTE

Covering sneezes and coughs reduces the chance of infected people dispersing droplets into the air where they can spread to others.

Practicing good respiratory hygiene means:

- Covering your nose and mouth with an elbow or clean tissue when you cough or sneeze (and no spitting)
- Wipe or blow your nose on a clean tissue and dispose of the tissue hygienically
- If no tissues are available, cough or sneeze into your elbow rather than your hand
- Encouraging participants to use tissues when they sneeze or cough
- Providing the means for prompt disposal of used tissues in general waste
- If required, encourage the use of masks
- Encouraging participants and others in the workplace to practice hand hygiene.

4.0 PERSONAL PROTECTIVE EQUIPMENT

Workers must have access to PPE as well as any other resources necessary to maintain safe working practices.

4.1 GLOVES

Gloves must be worn:

- For procedures with a risk of exposure to blood or bodily fluids e.g. assisting a participant with toileting or applying basic first aid
- When touching equipment or surfaces that may encounter blood or bodily fluids
- When performing personal care procedures
- When performing blood glucose monitoring

- When caring for participants who have an infection spread by contact
- If the worker has broken skin, cuts or abrasions on their hand which may pose a risk to the participant
- When preparing food.

Remember:

- Gloves are not to be used as a replacement for good hand hygiene.
- Remove gloves when a care activity is finished, change gloves before starting a different care activity
- Dispose of used gloves immediately after use in a manner appropriate to the work environment.

4.2 GOWNS AND APRONS

Gowns or aprons are used to stop contamination of workers' clothes and skin such as when there is a risk of splashes or sprays of blood or bodily fluids.

When using gowns or aprons:

- Perform good hand hygiene before and after using them
- Remove and dispose of gowns or aprons as soon as care is completed in a manner appropriate to the work environment and participant waste management process.

Gowns or aprons can be used:

- When clothes may be exposed to blood or bodily fluids, but it is low risk that arms will be contaminated.
- When the worker's clothes might get wet (e.g. showering a participant)
- Only once.

4.3 FACE MASKS

In rare cases STEPS may encourage the use of face masks when providing support to participants.

Face masks protect the workers nose and mouth from sharing infectious agents and are used if there is a risk of:

- A spreading of airborne contaminants
- Droplets or aerosols
- Splashes or sprays of blood and bodily fluids.

When using face masks:

- Check the manufacturer's instructions before use
- Do not touch the front of the mask with your hands once the mask is in place
- Use the mask for the care of one participant only.
- When the activity is complete, discard mask and perform hand hygiene.

4.4 PROTECTIVE EYEWEAR

Protective eyewear protects a worker's eyes from exposure to infectious agents and is always recommended when there is a risk of:

- Droplets or aerosols
- Splashes or sprays or blood or body fluids.

When using protective eyewear:

- Remember that the outside of the eyewear is contaminated
- When care is complete, remove eyewear using the headband or earpieces
- Clean eye shield after each use with detergent and water and allow to dry
- If eyewear is single use, dispose of after completion of care activity.

5.0 INCIDENTS AND SPILLS

5.1 MANAGING SPILLS

Prompt clean-up of spills (e.g. vomit or diarrhoea) helps to stop infectious agents spreading from the environment to people. When managing spills:

- Select the appropriate PPE such as gloves depending on the size of the spill
- Immediately wipe up spots and smaller spills and cover larger spills with absorbent material
- Dispose of contaminated cleaning materials
- Clean with detergent solution and consider following with disinfectant for infectious or larger spills
- Always perform good hand hygiene.

5.2 EXPOSURE TO BLOOD OR BODILY FLUIDS

If, during the provision of supports and services to participants, a worker comes in contact with blood or bodily fluids, the following steps are to be taken:

- Flush the area with running water
- Wash the area with soap and water
- Report the incident to the direct line manager
- Record the incident as per the Incident Notification Procedure (i090200)
- Seek medical advice.

If any clothes are contaminated, rinse the item under running water, soak in a bleach solution, then wash separately from other clothing or linen with hot water and detergent.

5.3 NEEDLE STICK INJURIES

During the course of work duties, workers may come into contact with needles or devices used for injections such as EPI Pens or insulin syringes or pens. Accidents can happen and needle stick injuries can occur.

Where this happens, the following process is to be observed:

- Immediately wash the affected area with soap and water
- If the skin is penetrated, wash the area with soap and water; apply a mild antiseptic, then cover the wound with a band aid or dressing

- Report the incident to your direct Manager or Team Leader
- Record the incident as per the Incident Notification Procedure (i090200)
- Seek medical advice.

5.4 SHARPS DISPOSAL

- All used sharps must be placed in a clearly labelled, puncture resistant container that complies with Australian Standard AS 4031 or AS/NZS 4261 immediately after the procedure is completed
- Wear disposable gloves at all times when handling any type of sharp object which may be infected with blood or body fluids
- Do not re-cap, break or bend sharps
- To pick up the needle or syringe, place the container beside the sharp that requires collection and pick up the syringe using tongs
- Place the sharp in the sharps container, sharp end first
- Sharps containers must not be filled beyond three quarters full
- Sharps containers must be disposed of by a waste disposal contractor according to respective State or Territory Government Regulations.

5.5 WASTE MANAGEMENT

Waste Disposal will be as per the State or Territory Legislation and Regulations. Where there are no specific State or Territory requirements in place the following applies:

- All Personal Protective Equipment including masks, gloves, aprons etc can be treated as general waste
- Clinical waste such as used swabs which do not contain expressible blood can be treated as general waste
- Used swabs must be:
  - Discarded into a leak-proof plastic bag
  - Kept out of reach of children
  - Disposed of as general waste.

6.0 CLEANING

Cleaning is an important part of stopping the spread of infection and depends on the objects involved and risk of contamination.

STEPS will ensure that all equipment is cleaned thoroughly and where possible use disposable towel and paper to limit the spread of infection.

When cleaning:

- Most surfaces can be adequately cleaned with warm water and detergent and an anti-bacterial multipurpose spray
- Allow cleaned surfaces to dry completely

- A detergent solution followed by disinfectant may be appropriate when an infection is known or suspected on surfaces of equipment.

7.0 HANDLING LINEN

To avoid spreading infectious agents from used linen:

- Wear appropriate PPE when handling linen of participants who have an infection and or are ill
- Place linen soiled with blood or urine or other body fluids into a leak-proof laundry bag/s. Do not carry soiled linen
- Do not sort or rinse used linen in areas used to provide support to participants
- Wash all linen using a good quality (if not anti-bacterial) laundry detergent and set the washing machine to use the highest possible hot water setting)
- Where possible, dry linen in a clothes dryer using the 'hot' setting
- Perform good hand hygiene after handling linen
- Store clean linen in a clean dry place, separate from used linen.

8.0 FOOD HANDLING AND PREPARATION

Safe food handling is important to prevent food-borne illness.

When handling food:

- Perform hand hygiene before putting on gloves and handling food
- Perform hand hygiene after using the toilet, coughing, sneezing, blowing nose, touching face, nose, ears or mouth, handling rubbish or after cleaning
- Avoid unnecessary contact with ready to eat foods
- Tie back long hair
- Do not sneeze, blow, cough over unprotected food or surfaces likely to encounter food
- Do not eat over unprotected surfaces likely to encounter food
- Do not touch food after touching body parts (hair, nose, ear, eye), skin lesions, saliva, mucus, sweat, blood, or money without first performing hand hygiene.

When preparing food:

- Keep hot food hot (above 60°C) and cold food cold (below 8°C)
- Use separate storage, utensils, and preparation surfaces for cooked and uncooked foods
- Wash all utensils and preparation surfaces thoroughly with hot water and detergent after use or place in the dishwasher and run the dishwasher cycle.

9.0 TRANSPORTING PARTICIPANTS

When transporting participants, care is required to reduce the risk of spreading infection. When transporting participants:

- Perform good hand hygiene before and after transport

- If a participant has a respiratory illness, encourage them to wear a mask and to perform respiratory hygiene/cough etiquette
- Sit separated if possible, i.e. have passenger use the back seat and sit in seat opposite driver side.

10.0 VIRUS PANDEMIC

STEPS will closely monitor outbreaks of potential pandemics and be prepared to take immediate steps to protect the health of its workers, customers, participants and students. STEPS will follow the instructions of both the World Health Organisation, Australian Federal Government and the Pandemic Response Guidance documents outlining the three Personal Protective Equipment escalation levels for Disability Accommodation Services, Community Health Services and In-Home Care Settings throughout the pandemic. Where STEPS, either directly or indirectly, has contact with individuals diagnosed with the virus during the pandemic, they will:

- Contact the applicable Public Health Unit for further advice and direction.
- Communicate regularly with their participants and workers to keep them informed of any possible impacts this may have on the provision of supports.
- Perform ongoing risk assessments on the risks involved in managing infectious/preventable diseases and outbreaks.
- Develop and implement a *Pandemic Management Plan* that specifically addresses business continuity, risk management to ensure continuity of supports and services where the workforce may be reduced, and resources limited.

11.0 TRAINING

Workers will be provided with training in accordance with their level of involvement with infection control processes.

12.0 RELATED DOCUMENTS

Document Name	Document Name
COVID 19 Vaccination Policy (i010116)	Incident Notification Procedure (i090200)

13.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	23 May 2024
Effective Date	28 June 2024	**Document Number**	i052000_v5_240628

(Uncontrolled when printed)

1.6.11 Managing a Workers' Compensation Claim

1.0 INTRODUCTION

All employees who injure themselves at work are entitled to submit a claim for workers' compensation through the relevant insurer. Following an injury, an employee eligible for workers’ compensation should be provided with the *Workers’ Compensation Claim form* to complete. In some cases, an employee may be provided the form by their treating medical practitioner, however, they must still advise their supervisor and provide a copy to them.

1.1 DEFINITIONS

Word	Definition
RRTWC	Rehabilitation and Return to Work Co-ordinator

2.0 MANAGING THE INJURY OR ILLNESS

Supervisors are primarily responsible for the management of an employee who has sustained an injury or illness at work. The supervisor will ensure that documentation, including medical certificates and appointments, suitable duties and support for the injured or ill employee are appropriately maintained throughout the process.

The supervisor will liaise with the RRTWC in order to complete the following steps and effectively assist in managing a workers’ compensation claim:

- Request from the employee the workers’ compensation medical certificate.
- Forward all relevant documentation, including medical certificates to the RRTWC.
- Diarise the end date of the current medical certificate, following up with the employee to provide a further medical certificate, on expiry of the current certificate.
- Complete all time and attendance records for injured employees, liaising with Payroll as required.
- Check medical certificates to determine whether the employee is able to return to work, with or without restrictions, liaising with the RRTWC to identify suitable duties and develop a Suitable Duties Plan (i090102) with the employee.

2.1 ROLE OF THE RRTWC

The role of the RRTWC is to support the supervisor and the injured employee to facilitate the Rehabilitation and Return to Work (i090100) procedure. The RRTWC will facilitate the process for claim management and provide supporting tools and coordination of key stakeholders, according to required timeframes, completing the following steps to effectively manage a workers’ compensation claim:

- Explain the claims process to the injured employee and assist with the completion of forms, as required.
- Complete the employer section of the relevant *Workers’ Compensation Claim form* in liaison with the supervisor.
- Coordinate the completion of the relevant W*orkers’ Compensation Claim form* and supporting documentation and submit to the insurer within the required timeframes.
- Liaise with the injured employee, their supervisor, treating medical practitioner and the insurer to develop a Suitable Duties Plan (i090102) and ensure sign off by all parties.

- Assist the supervisor to find suitable duties if none are available in the injured employee's normal work group.
- Provide a central point for liaison with the insurer, the supervisor, the treating medical practitioners and the injured employee to maximise successful return to work.
- Request written permission from the injured employee to discuss their restrictions with their treating medical practitioner to develop and review Suitable Duties Plan (i090102).
- Following commencement of the Suitable Duties Plan (i090102), regularly follow-up the application of the Suitable Duties Plan (i090102) with the injured employee and their supervisor.
- Liaise with the injured employee, supervisor, Payroll and the insurer to ensure accuracy of time and attendance records and payments, and that the insurer reimburses STEPS for wages paid while on sick leave or attending medical appointments.
- Update all relevant parties of any notification from the insurer on claim status.
- Create and maintain hard and soft copy files for each claim to mitigate any exposure for future legal action.
- Prepare monthly reports on rehabilitation and return to work activities to present to Executive Manager – Human Resources and ELT.

2.2 DEVELOPING A CASE FILE

For each workers' compensation claim a case file (in both hard and electronic format) should be created and maintained by the RRTWC and stored separately to the employee's file. The case file should include the following:

- case notes that document every conversation that takes place in relation to the claim.
- copies of all medical certificates.
- copy of signed Injured Worker Authorisation (i090101) form to speak to the treating medical practitioners.
- copy of the workers' compensation claim form.
- communication and documentation provided by the insurer; and
- copy of signed Suitable Duties Plan (i090102).

2.3 MAKING A WORKER'S COMPENSATION CLAIM

There are various insurers that cover STEPS employees' access workers' compensation as outlined below:

Location of STEPS workplace	Insurer
Queensland	WorkCover Queensland
Northern Territory, Tasmania, WA	CGU Workers Compensation

The RRTWC will be familiar with the notification requirements for each insurer and be able to advise supervisors and injured employees of these requirements when they are notified of an injury at the workplace.

Upon notification of a claim, the insurer is responsible for coordinating and monitoring all aspects of workers' compensation for which the insurer is liable following a workplace injury. They will liaise with the injured employee, treating medical practitioners and the RRTWC to facilitate a safe return to work, wherever possible. On claim acceptance, they will coordinate all relevant workers' compensation payments.

The costs associated with treatment of an injured employee by the treating medical practitioner can only be covered if the employee's claim is accepted. The employee must ensure that all receipts for treatment are kept to enable reimbursement if the claim is accepted. The employee must forward those receipts to their supervisor/RRTWC, who will forward them to the relevant insurer for reimbursement, should the claim be accepted.

Prior to claim approval, where the treating medical practitioner does not provide a clearance to return to full duties and directs that time off work is required, the employee will need to complete a leave application and take personal leave until the claim is decided. If the claim is accepted by the insurer, personal leave will be re-credited for any leave taken associated with the claim.

Medical appointments and treatments may occur in the employee's own time or during work time. If the appointments occur in work time, ensure this is recorded correctly on the time and attendance records.

Payments by the insurer will differ, depending on the insurer and the employee should be referred to their case manager at the insurer to discuss such matters.

3.0 CLAIM DENIED BY THE INSURER

Where a claim for workers' compensation is denied, the injured employee will still need to be managed under these procedures, based on the information available on their medical capacity.

4.0 APPEALING A CLAIM APPROVED BY THE INSURER

At times, STEPS may appeal an approved workers' compensation claim. In these cases, the RRTWC will escalate to the Executive Manager –Human Resources for consideration by the Managing Director/CEO to approve an appeal being lodged. The RRTWC will then follow the appropriate insurer's procedure for appeal.

Grievance Procedure

If an employee is unhappy with a decision regarding their rehabilitation, the employee should raise the matter with the RRTWC and then the Executive Manager – Human Resources. If the matter is still unresolved the employee can follow the Employee Grievance (e210100) procedure. If the employee remains unhappy with the decision following this procedure, the employee can request that the Case Manager appointed by the insurer becomes involved to assist in resolving the grievance.

5.0 COMMON LAW CLAIMS

The Executive Manager - Human Resources will manage common law cases in a timely and efficient manner, working with the relevant insurer and ELT member.

6.0 LONG TERM INJURY OR ILLNESS

Long-term injuries or illnesses can be difficult. There will come a time when the insurer finalises the workers' compensation claim and the employee may not be able to return to their pre-injury role at the time of claim finalisation. STEPS is required by legislation, to provide suitable duties for up to a year after injury. After that time, if the employee can't return to their pre-injury role, a process will be put in place to assist the employee with other employment options, either within STEPS, or external to STEPS.

7.0 EMPLOYEE SUPPORT

STEPS provides an Employee Assistance Program (EAP) to all employees which provides access to professional and confidential counselling services for work-related or personal issues. As part of an injured employee's medical treatment, they may be referred to a psychologist or other related medical practitioner, however, any employee involved in returning to work from injury is encouraged to access these services provided through STEPS EAP.

8.0 RELATED DOCUMENTS

Document Name	Document Name
Employee Grievance (e210100)	Injured Worker Authorisation (i090101)
Rehabilitation & Return to Work (i090100)	Suitable Duties Plan (i090102)
Workers Compensation Claim Form (GP)	

9.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	11 April 2024
Effective Date	24 April 2024	**Document Number**	i090600_v2_240424

(Uncontrolled when printed)

1.6.12 Managing Suspected or Confirmed Cases of Infectious Diseases

1.0 INTRODUCTION / GENERAL

STEPS is committed to providing and maintaining a safe work environment and adequate facilities for workers in carrying out their work, so far as is reasonably practicable.

To achieve this, STEPS will follow the advice of State and Territory Governments and public health authorities to limit the spread of infectious diseases. Infectious diseases are diseases caused by pathogenic microorganisms, such as bacteria, viruses, parasites, or fungi; these diseases can be spread, directly or indirectly, from one person to another. Examples include but are not limited to: Coronaviruses (such as COVID-19), Influenza (flu) and Respiratory Syncytial Virus (RSV) to workers, customers, participants, and students, as well as the community.

Primary responsibility for the prevention and control of infectious diseases lies with individuals.

2.0 STANDARD PRECAUTIONS

All people in attendance at a worksite must practice standard precautions including:

- hand hygiene
  - hand washing with soap and water
  - using antimicrobial hand rubs (for example, an alcohol-based hand rub).
- the use of personal protective equipment (for example, gloves and masks).
- respiratory hygiene
  - covering the mouth and nose when coughing or sneezing
  - using tissues and disposing of them appropriately
  - attending to hand hygiene immediately after coughing, sneezing or blowing nose.

Where roles have been identified as requiring personal protective equipment (PPE) this will be provided and supported by information and training on how and why the workers will be required to use them.

3.0 STAY AWAY FROM THE WORKPLACE

Workers have a duty to take reasonable care for their own health and safety and to not adversely affect the health and safety of others. For this reason if a worker becomes unwell, they must stay away from the workplace.

The worker must, as soon as reasonably practicable, inform their direct line manager of their inability to attend work. This should occur during the ordinary hours of the first day or shift where they felt unwell.

The worker must advise their direct line manager even when working remotely. Personal (sick) leave can be accessed if an employee is feeling unwell.

In some cases, the relevant Executive Leadership Team Member may approve remote working.

4.0 DIRECTING A WORKER TO GO HOME

A manager must require workers to leave the workplace if they are unwell.

In instances of flu-like symptoms, the worker may be advised to test for COVID-19 when they return home and advise the results to their manager. This is required to ensure that STEPS can provide a safe working environment.

The employee will be able to access their personal leave entitlements while unwell.

5.0 COVID-19

5.1 RESPONSE

To assist with the management of COVID-19, STEPS has developed:

- JSEA Template (i050104) located in the O: drive, WHS folder and Risk Assessments-JSEAs folder.

5.2 TESTING FOR COVID-19

Where a worker undertakes a test for COVID-19 and the test result is **positive**, the worker must follow current government advise which can be found on the following websites:

Queensland - First steps if you have COVID-19 | Health and wellbeing | Queensland Government (www.qld.gov.au)

Tasmania - Information for positive cases | Coronavirus disease (COVID-19)

Northern Territory - Tested positive to COVID-19

Where a worker undertakes a test for COVID-19 due to feeling unwell and the test result is **negative**, the worker can return to work when they are feeling well again.

5.3 CLOSE CONTACTS

Where a worker is a close contact, they must follow current government advice and advise their manager:

Queensland - Close contacts - coronavirus (COVID-19) | Health and wellbeing | Queensland Government (www.qld.gov.au)

Tasmania - Advice for contacts | Coronavirus disease (COVID-19)

Northern Territory - Close contacts | Coronavirus (COVID-19)

5.4 RETURNING TO WORK AFTER COVID-19

If you have tested positive for COVID-19 you can return to work in accordance with government advice which can be found as indicated below:

Queensland - After having COVID-19 | Health and wellbeing | Queensland Government (www.qld.gov.au)

Northern Territory - I tested positive for COVID-19 – First steps | Coronavirus (COVID-19) (nt.gov.au)

Tasmania - Tested positive to COVID-19

6.0 RELATED DOCUMENTS

Document Name	Document Name
Disability Services in Accommodation (i052300)	JSEA Template (i050104)

7.0 GOVERNANCE

Document Owner	Executive Manager – Human Resources	**Approval Date**	23 May 2024
Effective Date	27 May 2024	**Document Number**	i051900_v6_240527

(Uncontrolled when printed)

1.6.13 Noise Management

1.0 INTRODUCTION

The purpose of this procedure is to provide guidelines and information to effectively manage exposure to noise hazards and risks at STEPS Group Australia (STEPS) workplaces.

1.1 DEFINITIONS

Daily Noise Exposure Level	The summary of the various levels of noise experienced plus the time for which a person is exposed to each noise level throughout the working day.
Decibel (dB)	The unit for measuring sound levels.
Ear Muffs	A device which fits firmly over and completely covers the ears.
Ear Plugs	A device which fits into an ear canal.
Excessive Noise	A level of noise above an 8 hour equivalent continuous A-weighted sound pressure level of 85dB (A) or continuous C-weighted peak sound pressure level of 140dB(C).
Noise Exposure	The amount of sound energy the unprotected ear of a person is exposed to, given a $L_{Aeq,8h}$ or as L_{Peak}.
Noise-Induced Hearing Loss	Hearing impairment arising from exposure to excessive noise at work. Occupational noise-induced hearing loss is also commonly known as industrial deafness.
Sound	Small fluctuations in the air pressure that result in a wave capable of exciting in a listener the sensation of hearing.
Sound Level Meter (SLM)	An instrument consisting of a microphone, amplifier and indicating device, having a declared performance, and is designed to measure a frequency-weighted and time-weighted value of the sound pressure level.
Sound Pressure Level (SPL)	The relative magnitude, of sound pressure customarily expressed in decibels referenced to 20 Micro Pascals.

1.2 RESPONSIBILITIES

Executive Leadership Team will:

- Ensure that sufficient resources are allocated to ensure compliance and fully implement this procedure.

Supervisors will:

- Ensure workers are supplied with suitable Personal Protective Equipment (PPE) and are instructed in the correct fitting, use of, maintenance and storage of PPE; and
- Ensure workers wear PPE when exposed to excessive noise (as determined through noise surveys and indicated through signage, procedures or warnings).

Workers will:

- Follow any instructions given to them for health and safety in relation to noise and the use of noise management tools;
- Wear any PPE provided by their supervisor or STEPS;
- Appropriately maintain PPE that has been provided to them for use;
- Obey 'Mandatory Signs' where displayed;
- Always be aware of other persons in the near vicinity when using noisy tools and equipment and make them aware of the protective equipment to be used;
- Inform the supervisor immediately if PPE is damaged/in need of replacement or if they have any concerns/problems; and
- Report hazards/risks in relation to noise management to their supervisor.

2.0 GENERAL INFORMATION

Hazardous noise can affect a person's hearing and make it difficult to hear sounds necessary for working safely e.g. warning signals and communication. The amount of damage caused by noise depends on the total amount of energy received over time. This means as noise becomes louder it causes damage in less time.

Sound pressure level is measured in decibels (dB) and exposure is recorded as:

- For a work day '8 hour equivalent continuous' in daily noise exposure level; and
- The 'loudest noise' which is called a peak level.

The national standard for exposure to noise at work is an A-weighted sound pressure level; LAeq, 8h 85dB (A). Exposure to a noise level of 85dB (A) over an eight-hour period equals a daily noise exposure level of 1. Long term exposure to a daily noise exposure of less than 1 does not result in permanent hearing loss.

For peak level noise, the national standard is a C-weighted peak sound pressure level of 140dB(C). Exposure to levels of noise above peak sound pressure level of 140dB(C) can cause immediate damage.

3.0 IDENTIFYING NOISE HAZARDS

Supervisors and Health and Safety Representatives (HSRs) are to inspect the workplace to detect possible noise hazards as part of the Office Workplace Inspection. If a noise hazard is identified, complete the Noise Hazard Identification Checklist (i051501).

Where it is possible, immediate action to control noise should be taken.

Workplaces are to work towards an exposure limited of 85dB (A). This means that a worker's unprotected ears are not exposed to noise levels above daily noise dose of 1 (i.e. 85dB (A) during an 8 hour shift).

3.1 REVIEW AVAILABLE INFORMATION

Before conducting noise assessments, information on the noise levels of plant and equipment should be gathered from:

- manufacturers and suppliers;
- previous workers' compensation claims for hearing loss; and
- regulators, HSRs and technical specialists

3.2 ASSESS THE RISK

Where noise exposure has been identified as a risk or hazard and information cannot be sourced from the above options, a noise assessment needs to be done by a competent person in accordance with the procedures in *AS/NZS 1269.1 Occupational noise management: Measurement and Assessment of Noise Emission and Exposure.*

3.3 NOISE ASSESSMENT

A noise assessment should consider:

- type of workplace, number of persons at risk and information already gathered;
- all plant, equipment, tools and other sources of noise in operation (unless information is already recorded);
- the noise exposure levels produced during various tasks carried out during a working shift;
- how long the workers are exposed to noise during each of these tasks,
- the length of shift, and,
- environment factors (e.g. types of walls, surfaces, layout of work stations).

3.4 IMPLEMENT NOISE CONTROL MEASURES

Noise assessment results will determine what control measures are appropriate to take.

Control measures are to be carried out using a noise management plan. The plan should include specifications for use of protective equipment, purchasing/hiring of plant and equipment, scheduled audiometric testing, training needs and timeframes for review. Noise control measures selected should be appropriate in accordance with the Work Health and Safety Regulations.

Once the control measures have been implemented, regular review should occur as part of the scheduled inspection process to ensure the risks have been effectively controlled or eliminated.

4.0 PROCUREMENT PROCESS

The person in control of the procurement process should consider worker's exposure to noise levels when purchasing or hiring plant and equipment, with noise one of the items to consider when undertaking a Pre-Purchase Risk Assessment for Plant (i080102). Plant should be purchased or hired from suppliers who can demonstrate a low noise design, with noise control as a standard part of the machine, not as an optional extra.

5.0 PERSONAL PROTECTIVE EQUIPMENT (PPE)

PPE should be used in the workplace;

a) When risks from exposure to noise cannot be elimination or minimised by other more effective measures;

b) As an interim measure until other control measures are implemented; or

c) Where extra protection above what has been achieved is required.

PPE needs to be:

a) Suitable for the nature of work;

b) Suitable size and fit and reasonable comfortable; and

c) Maintained, repaired or replaced effectively

Signs are to be used accordance with *AS 1319 Safety signs for the occupational environment*. All employees, including visitors must be able to recognise situations when PPE are required. Where practical, signs should be attached on tools, equipment and plant.

6.0 AUDIOMETRIC TESTING

Any employee likely to be exposed to noise in excess of the current exposure standard is to undergo regular audiometric testing (at least every two years). Employees who are exposed to high $L_{Aeq,8h}$ (greater than 100 dB(A)) will undergo more frequent testing (e.g. every six months).

Any employee who wants to request a hearing test should discuss the matter with their immediate supervisor and Work Health and Safety Officer.

All employees who undergo audiometric testing are to be provided with the results of the test, with a written explanation of the meaning and implications. The results are confidential and will be saved on the employee’s record on the Human Resources Information System (HRIS), ConnX,

7.0 TRAINING

STEPS will ensure information, training and instruction are provided to all employees and others in the workplace on the health and safety risks associated with noise exposure.

Training will be provided to:

- Workers who are exposed to hazardous noise or other agents which may contribute to hearing loss;
- Their supervisors;
- HSRs; and
- Those responsible for purchase/ hire of plant, noise control equipment, PPE, and for the design, scheduling, organisation and layout of work.

Training and attendance records will be saved under the WHS folder of the network or in ConnX as required.

8.0 RELATED DOCUMENTS

Document Name	Document Name

5.15.1 Noise Hazard Identification Checklist (i051501)	8.1.2 Pre-Purchase Risk Assessment for Plant (i080102)
AS/NZS 1269.1 Measurement and Assessment of Noise Emission and Exposure	AS 1319 Safety Signs for the Occupational Environment
AS/NZS 1269.0 Occupational noise management Overview and general requirements	Work Health and Safety Act 2011 (s19 & s22) (Refer to the 2.1.1 Legislative Register)
Work Health and Safety Regulation 2011 (s35, s44 & s56-s59) (Refer to the 2.1.1 Legislative Register)	Managing Noise and Preventing Hearing Loss at Work Code of Practice 2011 (Refer to the 2.1.1 Legislative Register)

9.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	06 October 2022
Date of Issue	10 October 2022	**Document Number**	i051500_v2_221010

(Uncontrolled when printed)

1.6.14 Personal Protective Equipment (PPE)

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) will ensure the appropriate selection, introduction, maintenance, training and use of personal protective equipment (PPE) is achieved in accordance with the specific identified risks involved in either the workplace or a work practice.

2.0 RESPONSIBILITIES

Executive Leadership Team will:

Ensure that sufficient resources are allocated to fully implement this procedure.

Supervisors will:

Ensure that, all requirements for PPE are appropriately assessed, and where necessary, personal protective equipment is maintained and made available to all workers and visitors along with appropriate training.

Ensure that workers and any visitors comply with all requirements for safe use of personal protective equipment.

Workers will:

Ensure personal protective equipment is used on tasks, which require such, and that the equipment is properly cared for, and maintained.

2.1 CIRCUMSTANCES FOR THE PROVISION OF PPE

STEPS will supply PPE as required in response to an identified hazard in either the workplace or a recommendation arising from a risk assessment.

2.2 PROVISION OF PPE

STEPS recognises that the provision of PPE is only determined as an acceptable control measure if other control measures designated in the Hierarchy of Controls are not appropriate or leave an unacceptable residual risk. PPE will be used in conjunction with other controls and never as the only control for managing risks associated with hazards identified.

2.3 PURCHASE AND SELECTION OF PPE

All Personal Protective Equipment (PPE) purchased must comply with the relevant legislative requirements in each State/Territory and the applicable Australian Standard.

All PPE selected must take into account the specific hazards encountered in the workplace or work practice.

Such equipment must also give appropriate consideration to comfort and must not restrict movement or vision or interfere with the function of other required PPE. Wherever possible, workers who are required to use the PPE shall be consulted in regard to selection, and where applicable, pilot trials will be established.

A record shall be maintained of all suppliers of approved PPE for each of the specific work areas or work practice/s using Trade and Independent Contractor Information Form (i030102).

2.4 ISSUE OF PPE

Personal Protective Equipment PPE will be issued in a controlled manner, with only approved PPE being available for issue.

All STEPS Group Australia workers required to use personal protective equipment will be trained in its application, use and maintenance.

Workers, once trained, will be responsible for the proper care and maintenance of all PPE assigned personally to them. A nominated person in each case will maintain other general use PPE. Personal protective equipment must be kept fit for use at all times.

2.5 USE OF PPE

All PPE is to be used in accordance with supplier instructions and as designated by procedures.

Job Safety Environmental Analysis (JSEA) Template (i050104) will detail the PPE required to be worn for each task requiring the apparatus.

Managers and supervisors must ensure that workers consistently comply with PPE requirements in specific work areas or work tasks.

2.6 STORAGE OF PPE

To ensure the efficiency and reliability of PPE, it is important that all PPE is stored in a manner consistent with the manufacturer’s care and storage instructions. Where PPE is assigned to workers, they will be personally responsible for the care and maintenance of the PPE.

2.7 INSPECTION AND TESTING

All personal protective equipment is to be regularly inspected for faults or damage. It must be repaired or replaced where required. Any damaged or faulty equipment is to be withdrawn from service and not used under any circumstances.

2.8 CONTRACTORS REQUIREMENTS FOR SUPPLY OF PPE

All contractors, or their workers and representatives, who are required to undertake tasks on STEPS Group of Companies premises or sites, shall wear applicable PPE for that task. The contractor shall provide the PPE.

2.9 REVIEW OF PPE REQUIREMENTS

PPE requirements for each work activity and job position will be reviewed:

- After an incident where PPE is cited as one of the contributing factors;
- At review of a risk assessment, safe work procedure; or
- At two yearly intervals.

3.0 RELATED DOCUMENTS

Document Name	Document Name
Corporate Risk Register *(i050102)* *Completed Corporate Risk Registers saved in relevant folder in 'I' Drive.*	Job Safety Environmental Analysis (JSEA) Template (i050104)
Trade and Independent Contractor Information Form (i030102)	

4.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources Manager	**Approval Date**	17 December 2021
Effective Date	12 January 2022	**Document Number**	i050200_v3_220112

(Uncontrolled when printed)

.

1.6.15 Rehabilitation and Return to Work

1.0 REHABILITATION AND RETURN TO WORK

STEPS Group Australia (STEPS) is committed to ensuring an injured employee is returned to safe, productive and fulfilling employment as soon as possible. In order to achieve this STEPS will provide occupational rehabilitation, designed in conjunction with the employee and their treating medical practitioner, for an employee who incurs a work related injury or illness.

In situations where an employee sustains a non-work related injury or illness, STEPS is committed to exploring opportunities to provide rehabilitation (e.g. suitable duties), but in order to maintain ongoing operational viability, STEPS cannot guarantee this will be available or sustainable in all cases.

This procedure outlines the process to be followed for managing an injured employee and assisting to ensure that the employee is able to undertake appropriate treatment and be engaged in a suitable duties program to enhance a full return to work at the earliest opportunity.

1.1 RESPONSIBILITIES

Executive Leadership Team (ELT) and Program Managers will:

- Provide support and the resources to assist manager/supervisors to facilitate the rehabilitation and return to work of an injured or ill employee.
- Appoint an appropriately qualified Rehabilitation and Return to Work Coordinator (RRTWC) who has the qualifications, experience and/or standing appropriate to perform the function or exercise the powers of the role.
- Recognise the varying legislative requirements in meeting STEPS obligations under this procedure
- Ensure employees are educated to ensure they are aware that, in the event of injury or illness, they will be consulted to ensure a structured and safe return to work that will not disadvantage them.

Manager/supervisors will:

- Create a seamless transition from incident management through to the effective delivery of these rehabilitation and return to work procedures.
- Educate injured employees on this procedure and supporting processes.
- Establish regular contact with injured employees, providing assistance and support throughout the rehabilitation and return to work procedures.
- Regularly liaise with the RRTWC whilst carrying out all of the rehabilitation and return to work procedures.
- Ensure employees participating in the rehabilitation process are treated with confidentiality, respect and equity.

Injured employees will:

- Follow the relevant process for applying for workers’ compensation.
- Attend medical examinations, advising their treating medical practitioner of the availability of workplace rehabilitation and provide any supporting documentation or information to assist in the provision of suitable duties.
- Actively participate in workplace rehabilitation and all workplace efforts for an early return to work.
- Maintain communication with their manager/supervisor and the RRTWC in relation to their return to work, rehabilitation and any related compensation claim.

1.2 RETURN TO WORK AFTER INJURY

An unnecessary delay in returning to work, following injury, is often associated with delayed recovery and the longer an employee is away from work, the less chance they have of ever returning. STEPS commitment to facilitating a smooth transition back to the workplace can help employees stay active after injury, reduce pain symptoms and help employees return to their usual activities at home and at work sooner, benefiting the employee and the organisation.

An injured employee cannot come back to the workplace until they have a Medical Clearancee stating they are fit to resume work, either back to their normal role or with restrictions. STEPS recognises that return to work after time off can be difficult. The employee will need support and may need a graduated return to work. The manager/supervisor will need to liaise with the RRTWC as soon as confirmation is received that the employee is returning to work.

Where the medical certificate indicates they are fit to return to work, the employee should resume normal duties from that time. Where the certificate indicates the employee is able to return to work but has restrictions in place, the manager/supervisor should liaise with the RRTWC to establish a Suitable Duties Plan (i090102). Employees are required to make every reasonable effort to return to work. This includes participating in the return to work plan, assessments of work capacity and progress. If an employee does not make this effort, benefits could be stopped by the insurer.

It is the manager/supervisor's responsibility to remain in regular contact with the injured employee. The manager/supervisor should ask if they would like someone to call in on them, keep them up to date with any workplace activities or changes and ensure timely follow-up when they are due for review with the treating medical practitioner and obtain current medical certificates.

1.3 SUITABLE DUTIES PLANNING

A Suitable Duties Plan (i090102) will be developed by the RRTWC, in conjunction with the manager/supervisor and information provided by the treating medical practitioner and the employee. The manager/supervisor is responsible for sourcing alternate duties for the injured employee. An external provider, such as an Occupational Therapist, may be called in to develop the plan, if required. The plan will be developed following the recommendations made by the treating doctor.

The manager/supervisor and the employee will need to sign the plan to indicate both parties are responsible for ensuring the SDP is followed and the employee is not put at risk of aggravating the injury. In some cases, the employee may be deployed temporarily to another work area, and in these situations, the manager/supervisor of that area is responsible for time and attendance records and for the day-to-day management of duties in accordance with the Suitable Duties Plan (i090102). In such cases, the employee's regular manager/supervisor should keep in touch with the employee and the temporary manager/supervisor to monitor progress towards return to their normal work area.

The manager/supervisors involved in the Suitable Duties Plan (i090102), in collaboration with the RRTWC, should review the employee's progress regularly and upgrade duties in accordance with medical advice.

2.0 APPROVAL

All return to work plans require approval of the Managing Director/CEO.

3.0 RELATED DOCUMENTS

Document Name	Document Name
Suitable Duties Plan (i090102)	

4.0 GOVERNANCE

Document Owner	Human Resources Manager	**Approval Date**	5 October 2023

Effective Date	17 October 2023	**Document Number**	i090100_v3_231017

(Uncontrolled when printed)

1.6.16 Reviewing Work Health Safety (WHS) Status

1.0 INTRODUCTION

This procedure sets out the requirements for reviewing WHS status across all STEPS Group of Companies (STEPS) facilities and activities.

2.0 REVIEW OF WHS INSPECTIONS AND AUDITS FOR PREPARATION OF REPORT

The Work Health and Safety Officer (WHSO) is responsible for reviewing the following documents and records monthly to prepare the monthly Report to the Executive Leadership Team (ELT):

2.1 ALL INSPECTION RECORDS AND AUDIT REPORTS

All Inspection Checklists include instruction procedures.

Human Resources Teams	
Rectification Action Plan (i060202)	Rectification Action Plan – Creche (i060206)
Rectification Action Plan - Garden Centre (i060204)	WHS components of the Quality Objectives Plan (i010301)
WH&S Creche Inspection Checklist (i060205)	WH&S Garden Centre Inspection Checklist (i060203)
WH&S Office Inspection Checklist (i060201)	

2.2 REGISTERS

Human Resources Teams	
Incident Register (electronic) *Refer to WHS Officer*	

3.0 TREATMENT OF NON-CONFORMANCES ARISING FROM THE REVIEW

All non-conformances will be communicated to the relevant parties and recorded in the Organisational System Improvement (OSI) System.

4.0 RECEIPT OF FEEDBACK FROM EXECUTIVE MANAGERS AND DIRECTORS

Feedback from Executive Managers and Directors must be dealt with promptly to enable corrective actions and continued improvement strategies to be commenced.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Corporate Risk Register (i050102)	Incident Register (electronic) Refer to WHS Officer
Quality Objectives Plan (i010301)	Meeting Minutes Template (i040302)
Rectification Action Plan (i060202)	Rectification Action Plan – Creche (i060206)
Rectification Action Plan - Garden Centre (i060204)	WH&S Creche Inspection Checklist (i060205)
WH&S Garden Centre Inspection Checklist (i060203)	WH&S Office Inspection Checklist (i060201)

6.0 GOVERNANCE

Document Owner	Executive Manager Human Resources	**Approval Date**	7 August 2024
Effective Date	1 October 2024	**Document Number**	i060200_v3_230602

(Uncontrolled when printed)

1.6.17 Smoke Free Workplace

1.0 PURPOSE

The purpose of this procedure is to provide guidelines and information to ensure that STEPS Group Australia (STEPS) maintains a smoke free working environment so that STEPS meets its work health and safety obligations.

1.1 DEFINITIONS

Passive Smoking	Passive smoking means the inhalation by any person of air contaminated by tobacco smoke.

2.0 SMOKING IN THE WORKPLACE

STEPS is committed to providing a safe and healthy work environment for all workers. Smoking exposes people to hazardous chemicals and it can increase the risk of fire. Smoking is therefore prohibited in all buildings, office areas and certain other work areas that are designated ‘non-smoking’ areas including:

- Office, conference rooms, training areas, toilets, stairwells and fire escapes.
- Enclosed car parks.
- Basement areas.
- Storage facilities.
- Motor vehicles.
- Lunchrooms, cafeterias and recreation areas.
- Within 4 metres of an entry door or air intake system.
- Near any methane gas storage areas.
- Within 8 metres of flammable liquid being decanted (e.g. refuelling point).

2.1 RESPONSIBILITIES

All workers have the responsibility not to smoke and take all reasonable steps to avoid passive smoking in the work environment (including vehicles).

All workers share in the responsibility for adhering to and enforcing this procedure. Further, when working off-site workers must adhere to all relevant client site-specific policies and procedures regarding smoking and are only permitted to smoke in designated areas and during breaks. In addition, Managers and Supervisors will support workers to adhere and enforce this procedure and work with clients to minimise any identified risks.

2.2 CONSULTATION

Where possible, consultation will be ongoing with workers to ensure a smoke free work environment.

2.3 CONTROL MEASURES

‘Smoke Free Workplace’ signs may be displayed to show that smoking is prohibited in buildings and vehicles. STEPS will eliminate workers’ exposure to the effects of passive smoking, wherever possible and where this is not possible, STEPS will introduce effective controls to minimise any exposure.

Smoke alarms are installed in workplaces to alert workers of a fire. As tobacco smoke (being a combustion product) will set off these alarms, smoking is not allowed in buildings or in the near surroundings.

3.0 GUIDELINES WHEN WORKING IN A CLIENT'S HOME

STEPS recognises that the client's home is a workplace, which means that clients must provide, as far as reasonable, a safe working environment for workers coming into their home. As a workplace, this means that workers must never smoke in a client's home.

STEPS also recognises client's rights to make decisions and exercise choice, because of this STEPS does not want to restrict the rights of individuals to take part in a legal activity in their own homes, whilst ensuring they minimise worker exposure to second hand tobacco smoke.

Where a client exercises their rights to smoke in their home, workers must consult with the client to introduce an informal agreement that the client does not smoke in the presence of the worker, or where support occurs predominately outside the home, that the client smokes in a well ventilated area. Workers are also encouraged to consult with the client on ventilating rooms on arrival to remove existing smoke in the home.

Where a worker believes they are at risk, they must report this hazard to their Supervisor and a risk assessment can be conducted to develop a plan to manage the risk. The client should, wherever possible, be involved in conducting risk assessments and developing solutions.

Solutions to be considered include:

- Entering into a plan to quit smoking if this is the client's wish.
- Ask any clients who are visited regularly not to smoke for a certain period prior to any pre-arranged visit and during a visit.
- Ask the client not to smoke while the worker is present.
- Limit smoking to rooms where people will not be working and open windows in rooms where people are working to help clear second hand smoke.

Some workers may have a pre-exiting condition that may be made worse by exposure to tobacco smoke, such as asthma, chronic obstructive pulmonary disease or cardio-vascular disease, or who face additional risks e.g. during pregnancy. As workers with these conditions are at higher risk, particular care should be taken to prevent or minimise their exposure to tobacco smoke.

4.0 RELATED DOCUMENTS

Document Name
Nil

5.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	6 October 2022
Effective Date	10 October 2022	**Document Number**	i051200_v2_221010

(Uncontrolled when printed)

1.6.18 Work Health & Safety Management for Building Works

INTRODUCTION/GENERAL

Work Health and Safety (WHS) Legislation requires employers to provide for the health and safety of their employees.

This responsibility extends beyond an employer's own employees and includes other persons who may be required to work on the employer's premises or to persons who carry out work under the direction of a principal contractor.

STEPS Group of Companies (STEPS) will seek to ensure that trade contractors involved in building works have safe systems of work in place while performing work on behalf of STEPS.

1.1 DEFINITIONS

Word	Definition
Trade Contractors	Provide a trade service (including but not limited to, shop fitting, plumbing, building, electrical, tree lopping, ICT installers).
Building works	Construction, erection, demolition, extension, restoration, alteration, destruction, assembly or placement of any building structures, includes installation in any building including but not limited to heating, lighting, air conditioning, security and ICT systems.

1.2 RESPONSIBILITIES

For each building works, the Managing Director will nominate a STEPS Representative who will fulfil the responsibilities as outlined in 1.3 below. To satisfy WHS requirements, the STEPS representative will provide the trade contractor with the Trade & Independent Contractor Information (i030102) to complete and the Contractor WHS Obligation (i030201) to review. Upon return of completed documentation, the trade contractor will be added to the Register of Providers (i030101).

STEPS and its contractors should define which party is to take responsibility for control of the working area, systems of work, plant and equipment, hazardous chemical use, storage and disposal, induction training, supervision and resolution of issues etc.

When this has been decided, STEPS will ensure that all relevant parties are informed of the WHS arrangements.

1.3 SPECIFIC RESPONSIBILITIES

STEPS Representative

It is the responsibility of the STEPS Representative to seek to ensure that:

- WHS Management Plans, Safe Work Method Statements, Safe Work Procedures, Job Safety Analysis, Plant and equipment maintenance schedules and Risk Assessment documents are available prior to commencement of work.
- Any site specific rules are clearly communicated to the relevant parties.
- The primary contractor has successfully completed any prescribed contractor induction processes, including site induction prior to commencing work.
- Consultation and communication takes place between those planning the work, those contracted to carry out the work and those who will be impacted (office workers in occupied areas) by the work.
- Contact is maintained with the contractor throughout the building works.
- Liaise with STEPS WHS Officer as required.

Contractors

It is the responsibility of contractors to ensure that they:

- Are competent to do the job asked of them.
- Have the qualifications, training, experience and certificates of competency that will be needed for the job.
- Have the WHS knowledge required for the job.
- Follow any site specific rules communicated by STEPS.
- Raise any issue regarding hazards that is or may become a WHS concern.
- Employ safe tools and systems of work to do the job.
- Comply with relevant legislation, Codes of Practice and appropriate standards.
- Manage hazardous chemicals safely and provide Safety Data Sheet (SDS).
- Maintain the premises in which they work in a safe and healthy manner for themselves and for the employees and visitors of STEPS.
- Communicate regularly with the STEPS Representative and STEPS WHSO as required.
- Report any serious workplace incidents to STEPS and the WHS Regulator.
- Undertake regular hazard inspections and site audits as agreed with the STEPS Representative or relevant supervisor and make these records available upon request.

2.0 ACCESS TO SITE – CONTRACTOR AND SITE VISITOR REGISTER

All contractors and visitors will be advised at first entry to site of the daily requirement to enter their details into the In/Out Register – Visitors/Contractors (i100203). All persons entering any STEPS site must sign in and out at each entry without exception. The register contains a list of persons on site in the event of an emergency.

3.0 WHS ORIENTATION

All contractors must be orientated to the STEPS site prior to commencing work. The orientation will be given by the STEPS Representative, Business Manager or a STEPS WHS Officer.

4.0 PROCEDURES FOR MONITORING AND REVIEW OF CONTRACTOR WHS PERFORMANCE

In the event the STEPS representative observes unsafe work practices, this will be brought to the attention of the contractor and both parties will work towards resolution of the issue. Observed improvement should be noted and made the subject of positive feedback to those involved or responsible.

Unplanned changes to the work environment that may impact on a particular activity will be communicated to those involved immediately. Planned changes to work conditions or environment will be communicated to the STEPS Representative.

The contractor will report any WHS incidents and rectifications to the STEPS Representative and WHS Officer Non-compliances will be recorded and the persons responsible to close out the action will be notified.

4.1 INSPECTIONS

Where building works are undertaken within the workplace and cannot be separated from STEPS, the STEPS Representative or WHS Officer will attend regular inspections with the contractors. The STEPS Representative or WHS Officer will provide feedback to contractors and workers, including STEPS Health & Safety Representatives (HSRs) on the performance of the works and any issues arising from the inspection.

5.0 RECORDING INCIDENTS

The contractor will record any incidents that require corrective action or notification for rectification of work process, repairs, or replacement of plant and these will be reported to the STEPS Representative and STEPS WHS Officer.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Contractor WHS Obligation (i030201)	Health, Safety and Environment Policy (i010101)
In/Out Register - Visitors/Contractors (i100203)	Register of Providers (i030101) *Refer to the Quality Assurance & Risk team*
Trade & Independent Contractor Information (i030102)	

7.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	16 November 2023
Effective Date	30 January 2024	**Document Number**	i030200_v2_240130

(Uncontrolled when printed)

1.6.19 Working Alone and Isolated Work

1.0 PURPOSE

This procedure gives effect to the requirements for those workers who are required to work alone or perform isolated works.

1.1 DEFINITIONS

Term	Meaning
Isolated Work	In relation to a worker, means work that is isolated from the assistance of other persons because of location, time or the nature of the work.
Assistance	Includes rescue, medical assistance and the attendance of emergency service workers.

2.0 WORKING ALONE AND ISOLATED WORK

STEPS recognises its duty to manage the risks associated with working alone and isolated work, including ensuring effective communication with workers.

Examples of working alone and isolated work include:

- Workers on call after hours
- Support Workers
- Contract Cleaners

In some situations, a worker may be alone for a short time. In other situations, the worker may be on their own for a shift, including sleepovers at client's premises.

2.1 ASSESSING THE RISKS

Working alone or remotely increases the risk of any job. Exposure to violence and poor access to emergency assistance are the main hazards that increase the risks when working along or isolated work. The following factors should be considered when assessing the risks:

- Mobile phone / radio / or satellite contact is available at all times.
- The off-site work is planned and rest breaks are factored in.
- Designated contact times with supervisor have been established.
- Is the work in a remote location that makes immediate rescue or attendance of emergency services difficult? If so, refer to the Remote Travel Procedure (i051000)
- Are you aware of the emergency procedure e.g. fire evacuation and cyclone procedures.
- What is likely to happen if there is a vehicle breakdown?
- I know how to use the required machinery, tools and equipment?
- Is fatigue likely to increase risk, e.g. driving long hours in a vehicle?
- Is there a risk of violence or aggression when dealing with this client or customer?
- Can environmental factors effect the safety of the worker, e.g. exposure to extreme hot or cold environments?
- Is there risk of attack by an animal, e.g. reptiles or insects?
- I have the skills and capabilities, experience and training to make sound judgements about safety in this environment?
- Do you have a pre-existing medical condition that may increase risk?

3.0 CONTROLLING THE RISKS

Buddy system

Where appropriately assessed and funding provided duplicate employees may be rostered to minimise risk.

Workplace layout and design

Workplaces and their surrounds can be designed to reduce the likelihood of violence, for example ensure access to exits is clear of any obstructions.

Communication systems

- The type of system chosen will depend on the distance from the base and the environment in which the worker will be located or through which he or she will be travelling. Expert advice and local knowledge may be needed to assist with the selection of an effective communication system.

- If a worker is working alone in a workplace that has a telephone, communication via the telephone is adequate, provided the worker is able to reach the telephone in an emergency. In situations where a telephone is not available, a method of communication that will allow a worker to call for help in the event of an emergency at any time should be chosen, for example:
    - Personal security systems, being wireless and portable, are suitable for people moving around or checking otherwise deserted workplaces. Some personal security systems include a non-movement sensor that will automatically activate an alarm transmission if the transmitter or transceiver has not moved within a certain time.
    - Radio communication systems enable communication between two mobile users in different vehicles or from a mobile vehicle and a fixed station. These systems are dependent upon a number of factors such as frequency, power and distance from or between broadcasters.
    - Satellite communication systems (e.g. SPOT devices) enable communication with workers in geographically remote locations. Satellite phones allow voice transmission during transit, but their operation can be affected by damage to aerials, failure of vehicle power supplies, or vehicle damage.
    - Distress beacons should be provided where life-threatening emergencies may occur, to pinpoint location and to indicate by activation of the beacon that an emergency exists. Distress beacons include Personal Locator Beacons (PLB) for personal use.
    - Mobile phones cannot be relied upon as an effective means of communication in many locations. Coverage in the area where the worker will work should be confirmed before work commences. Geographical features may impede the use of mobile phones, especially at the edge of the coverage area, and different models have different capabilities in terms of effective range from the base station. Consult the provider if there is any doubt about the capability of a particular phone to sustain a signal for the entire period the worker is alone. If any gaps in coverage are likely, other methods of communication should be considered. It is important that batteries are kept charged and a spare is available.
    - Movement records – knowing where workers are expected to be can assist in controlling the risks, for example call-in systems with supervisors or colleagues. Satellite tracking systems or devices may also have the capability of sending messages as part of a scheduled call in system, and have distress or alert functions.

Training and Education

STEPS will provide training for all workers required to work alone or perform isolated works. For example, training in dealing with potentially aggressive clients, using communications systems, administering first aid, and obtaining emergency assistance.

4.0 WORKING ALONE AND ISOLATED WORK CHECKLIST

The Fatigue Management and Isolated Work or Working Alone Checklist (i050601) must be completed by each employee who will be working alone or performing isolated work prior to any works taking place with full communications system agreed to and signed off by the relevant parties. The Fatigue Management and Isolated Work or Working Alone Checklist (i050601) must be reviewed every 6 months or when an employee undertakes the works for the first time.

5.0 RELATED DOCUMENTS

Document Name
Fatigue Management and Isolated Work or Working Alone Checklist (i050601)

6.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	Approval Date	6 October 2022
Effective Date	10 October 2022	Document Number	i050600_v2_221010

Uncontrolled when printed

1.6.20 Work Health & Safety Incident Investigations

1.0 INCIDENT INVESTIGATION

Any Moderate, Major or Extreme incident, which involves injury, illness, or significant property damage, shall be investigated. There are also events usually referred to as 'near misses', or 'lucky escapes', such incidents have the same contributing factors as more serious incidents, only the outcomes vary. The investigation of these incidents will therefore help to identify factors, which will help to prevent incidents that affect the health and safety of workers and visitors occurring in the future.

The main aim of investigating incidents is to:

- Prevent similar incidents recurring.
- Identify causal hazards.
- Identify and choose suitable preventative control options.

STEPS Group Australia (STEPS) is committed to reducing damage to the environment and the cost in pain, suffering, disruption to work, and loss of earnings of all workers and visitors. The supervisor in consultation with the relevant Executive Leadership Team (ELT) member with assistance from the Work Health and Safety Officer (WHSO), will investigate fully and accurately the circumstances and contributing factors of incidents in order to develop systems and processes that are safe and without risk to the health and safety of workers and visitors.

Any contractor, contractor worker, or representative involved in an incident at a STEPS work location shall immediately notify the relevant supervisor.

This procedure shall apply in all instances, including where workers are working at premises not owned by STEPS.

Additional requirements for reporting and investigation of incidents may be required by the owner/occupier(s). These shall be documented at site level and carried out in addition to the requirements outlined in this procedure.

2.0 CONDUCT AN INVESTIGATION

It is critical that an investigation occurs as soon as possible after the incident. The less time that elapses between the incident and the ensuing investigation, the more accurate the information and details will be. While concern for any injured person shall take precedence over everything else, when incidents involving injury or illness occur, early investigation is essential.

Employees should verbally report the incident to the Supervisor as soon as possible after the incident occurs then, complete and lodge a WHS Incident Report (i090201) as soon as is practicable and within a maximum twenty four hours (24) of the incident.

A serious incident scene is not to be interfered with until directed by a WHS Inspector, unless the interference is to save a life, relieve suffering, or to prevent injury to a person or property damage.

Where First Aid is administered, a record should be made of the first aid management given and recorded on the WHS Incident Report (i090201).

An investigation may require photographs, sketches, or another's technical expertise before the final causes of an incident can be determined and adequate controls considered and chosen.

2.1 COMMENCING THE INVESTIGATION

- Make sure any injured person receives appropriate medical attention immediately by calling 000 or 112 from a mobile.
- Control the incident scene, place barriers, turn power off, etc.
- Start the investigation as quickly as possible.
- Conduct interviews at the scene of the incident if possible.
- Ensure that the witnesses discuss the incident in relative privacy. Begin with those who can contribute most.
- Give each witness copy of their statement to review and correct if required – it must be their words NOT yours.
- Request that each statement is signed and dated.
- Take immediate corrective action where warranted.
- Complete report with recommendations.
- Ensure follow-up action occurs.
- Consider the longer term preventive actions as well.

2.2 KEY ISSUES DURING THE INVESTIGATION AND INTERVIEWS

- Obtain the names of everyone involved, near, present, or aware of possible contributing factors.
- Describe materials and equipment involved, check for defects, get an exact description of chemicals involved, etc.
- Describe exact location; note all relevant facts, lighting, weather, floor conditions, etc.
- Note exact time, date and other factors, work cycle, break period, etc.

- Describe usual sequence of events and actual sequence of events before, during, and after the incident.
- Find all possible direct/indirect causes and recommend how to keep it from happening again.

2.3 FUNDAMENTAL CONCEPTS

- Causes of incidents are rarely simple when circumstances are examined closely.
- Behind every incident there are many contributing factors.
- The key is to identify those that can be most effectively acted upon to prevent recurrences in the long term.
- Investigations should concentrate on the long-term elimination of injury, loss, or damage. The focus should be on systems deficiencies, in preference to human factors.
- After identifying causes and factors, suitable improvement actions must be identified, utilising the 'Hierarchy of Controls', and implemented by the dates set.

3.0 INVESTIGATION STEPS AND ESCALATION PRIORITIES

The supervisor of the person/s involved in the incident should ensure that the scene is left undisturbed until the investigation is completed. All incidents must be reported in accordance with the requirements of the Incident Notification Procedure (i090200).

- All incident investigations should be completed within 24 hours.
- A statement from the injured worker may be collected at a later date, if necessary.
- All incident investigations must be thorough, with sufficient detail to enable an accurate assessment of the circumstances to ensure appropriate action is then taken.
- All relevant sections of the WHS Incident Report (i090201) must be completed.
- Incident reports will be forwarded to WHSO for review.

Please note that in completing the investigation requirements, the incident investigation forms will need to remain active until the corrective action is completed and the review has been undertaken.

A copy of the WHS Incident Report (i090201) should be maintained at the relevant workplace or site, with the original forwarded to whs@stepsgroup.com.au.

The WHS Officer/Executive Manager – Human Resources will be responsible for ensuring that all parties are fully involved in the investigation and liaise with WHS Inspectors as required.

4.0 INVESTIGATION TEAM

When an investigation team is required to be assembled, the Executive Manager – Human Resources shall identify a team to be responsible for undertaking the investigation. This team shall be selected based on their training, and knowledge of the workplace or work practice. The WHSO shall be included as part of that team, as will the relevant Health and Safety Representative (HSR).

5.0 INCIDENT INVESTIGATION GUIDELINES

During the investigation the following shall be undertaken:

- A complete analysis of the incident details. Refer WHS Incident Report (i090201) including details of what happened, where it happened and what was involved (e.g. substances, products. equipment models, etc.).
- Appropriate corrective action must be established and taken to prevent recurrence. Proposed action must be outlined to address each contributing factor. Responsibility for actions must be delegated and a date for completion assigned.
- Corrective action is to be determined using the Hierarchy of Control Options. Refer Risk Management (i050100).
- All corrective actions identified must be indicated on the WHS Incident Report (i090201) and the WHSO will report on any outstanding/overdue corrective actions on a monthly basis. The WHSO will review the Rectification Action Plan (RAP) (i060202) form as at the date set. The WHS Incident Report (i090201) is considered a live document until this review process has been undertaken.
- Each incident and its review shall be entered into the Incident Register by the WHSO following an incident the relevant risk assessment will be reviewed by the WHSO.

6.0 TRAINING

All persons required to be involved in undertaking incident/incident investigations shall be trained and this training shall be recorded in either the Human Resources Information System (HRIS) ConnX, or electronically in the Human Resources files.

7.0 RECORD MAINTENANCE

Records of all incident and incident notification, investigation and corrective actions shall be maintained in accordance with the Records Management Archiving Procedure (i020300).

8.0 RELATED DOCUMENTS

Document Name	Document Name
Incident Notification Procedure (i090200)	Incident Register – *Refer WHS Officer*
Records Management Archiving Procedure (i020300)	Rectification Action Plan (RAP) (i060202)
Risk Management (i050100)	WHS Incident Report (i090201)

9.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	17 October 2023
Effective Date	3 November 2023	**Document Number**	i090300_v4_231103

(Uncontrolled when printed)

1.7 Client Service Management

1.7.1 Advocacy

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) encourages all participants receiving STEPS services including job seekers and students to utilise the service of an advocate of their choice to not only support their current and ongoing needs but ensure they receive the best possible service.

The purpose of this procedure is to provide guidelines to employees to ensure:

- The advocacy rights of our participants are consistently respected;
- A consistent approach to informing participants of this right; and
- A consistent approach in facilitating this process on the participants behalf when this option is chosen.

1.1 DEFINITIONS

Advocacy	**Advocacy** for people with disability can be defined as speaking, acting or writing with minimal conflict of interest on behalf of the interests of a disadvantaged person or group, in order to promote, protect and defend the welfare of and justice for either the person or group by: • Acting in a partisan manner (i.e. being on their side and no one else's); • Being primarily concerned with their fundamental needs; • Remaining loyal and accountable to them in a way which is empathic and vigorous (whilst respecting the rights of others); and • Ensuring duty of care at all times.
Formal Advocate	**Formal Advocates** are appointed with respect to legislation and therefore with the legal power to act on the participants behalf.
Informal Advocate	**Informal Advocates** are appointed by the participant and therefore provide information, advice and support but the decisions are ultimately made by the participant.
Professional Advocate	**Professional Advocates** are advocacy organisations that act on behalf of an individual or group of individuals.

2.0 GENERAL

All participants and potential participants may involve an advocate to represent their interests at any time as accepted practice by STEPS.

STEPS will:

- Offer each participant the opportunity to nominate an advocate.

- Accept the involvement of an advocate of the participants choice whenever this is the wish of the participant.
- Develop and maintain links with advocacy groups in all of its areas of operations and inform participants of the availability of such assistance.

2.1 EMPLOYEE RESPONSIBILITIES

Employees are to consult and negotiate with any participant-nominated advocate when making service decisions about the participant; will inform the advocate of any service changes; and will respect their legitimate role in any appeal or grievance proceedings.

3.0 PROVISION OF INFORMATION

Upon engagement with a participant, employees will advise participants that they are free to ask a family member, friend or other person to advocate on their behalf, and that STEPS welcomes the involvement of this advocate.

Our procedure on the use of advocates is made known to employees, volunteers, committee members and participants.

Information about the right to an advocate, and about advocacy services that may be able to assist the participant, is made available in written form as well as verbally.

Participants are made aware that they can change their advocate at any time.

Participants are to be reminded of their right to use an advocate on subsequent visits and contacts, along with their other rights associated with the services that they may receive.

4.0 APPOINTING AN ADVOCATE

Employees are to ensure that an Advocate Nomination Form – New/Change (i020402) is signed when an advocate is assigned this role by a participant/legal representative or the participant/legal representative has requested a change in advocate.

All participants and advocates are to be presented with a copy of the Advocate Guidelines (i020401) which outlines the role and responsibilities of an advocate.

Although STEPS employees will assist and support their participants in many ways, it is not appropriate for a STEPS employee to sign as the nominated advocate for a STEPS participant, due to a possible conflict of interest.

5.0 PARTICIPANT/CARER CONFLICT

In the case of participant/carer conflict, employees shall provide information to both parties on the availability of third party advocacy services.

6.0 ROLE OF AN ADVOCATE

Advocacy may involve speaking, acting or writing on behalf of an individual (or group) who has limited ability to exercise their rights.

Advocates may be requested to support the participant in their rights to:

- privacy and confidentiality;

- respect and dignity;
- quality services;
- information to inform decision making;
- choice and control;
- resolution of complaints;
- non-discrimination; and
- protection of legal and human rights and freedom from abuse and neglect.

Advocacy differs from mediation and negotiation. The role of the advocate is not impartial, as they have an obligation to operate entirely from the perspective of the participant in negotiating an outcome.

7.0 RELATED DOCUMENTS

Document Name	Document Name
Advocate Guidelines (i020401)	Advocate Nomination Form – New/Change (i020402)

8.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	3 November 2022
Effective Date	25 November 2022	**Document Number**	i020400_v2_221125

(Uncontrolled when printed)

1.7.2 Defensible Documentation Operational File/Case Note

1.0 INTRODUCTION

File/Case notes are a legal record that detail the care received by participants, their health, any important changes, participant's achievements, and movement towards their goals (as identified in their Support Plan). File/Case noting is integral to providing high quality service provision with the participant being the central focus. They represent a record of events on each shift or visit, and act as an important communication tool for staff and families. Ongoing and effective communication is essential as part of a team approach. This ensures participants safety and wellbeing where continuity of care is essential for effective service delivery.

STEPS actively promotes the implementation of **Defensible Documentation using the FACT® method** (Facts, Actions, Communication, Time/s). This is a best practice documentation method that a reader quickly understands, is legally compliant, contains factual information that minimises the likelihood of incidents, enables high-quality care, clear communication and provides the required information when care is questioned. It is a worker's responsibility to be aware of all relevant agency requirements.

Defensible Documentation provides evidence that quality care was provided by competent staff, it reflects our duty of care and provides evidence that:

- actions were informed by policy/procedure/care and support plan.
- action occurred to prevent harm in response to complaints, incidents, and foreseeable risks.
- service provision was directed/controlled/chosen by the client or nominee.
- dignity of risk was supported by informed decision making.

1.1 FILE/ CASE NOTES SERVE MANY PURPOSES:

- Provide professional **accountability** by providing evidence of actions, services and support being provided to clients.
- Demonstrate appropriate duty of care and responses to risk.
- Assist with planning and Case/File reviews.
- Meet service standards and requirements of funding bodies.
- Help guide staff in their role to fulfill their duties and implement participant goals.
- Assist in client handover.
- They are part of a client's permanent legal record. They may be used in legal proceedings, audits, and investigations.
- They provide a paper trail in case of conflict or incidents.

1.2 FILE/CASE NOTES IN REVIEWS/AUDITS

When developing an organisational response to a situation that has occurred all documentation is reviewed. File/Case notes provide background information that may be needed in any review/audit process. This includes:

- service improvements e.g., support strategies – what worked and what didn't.
- revealing patterns of behaviour/change over time.
- investigation into an incident.

This is where the importance of good record keeping is vital as it allows the organisation to formulate an accurate and comprehensive response where needed.

2.0 WHAT INFORMATION SHOULD BE INCLUDED IN A FILE NOTE

File/Case notes must be entered promptly upon completion of each shift by the person completing the shift and should be entered into the relevant participants Client Relationship Management system.

File/case notes should:

- Be written in the past tense.
- Be objective /factual – what is seen, heard, smelt, touched.
- Be legible and professional – blue/black ink if handwritten. Ensure the use of correct spelling and grammar.
- Be clear and concise.
- Contain relevant information - document information which provides evidence of duty of care.
- Be jargon free – Avoid words others may have trouble understanding and abbreviations / acronyms.

- Be concise - keep sentences short and to the point. Use dot points for clarity.
- Only use terminology that staff in your service use and understand.
- Not make reference to any other person receiving services from STEPS to avoid any privacy breaches.

Include only relevant Information

- When writing File/Case notes, ask yourself whether the information you are entering is relevant and, if so, for what purpose.
- Avoid adding unnecessary/superfluous detail, this makes reading File/Case notes lengthy, and it is hard to pick out the pertinent information. **Use dot points for clarity.**
- Relevant information pertaining to each and every support shift needs to be recorded. 'If it's not written down, it didn't happen'.
- It is important to always be mindful that File/Case notes may be read by others, whether the clients themselves, their family or by legal practitioners and courts.

Dignity and respect

The tone and selection of words used in File/Case notes convey a powerful message. Remember that:

- File/Case notes should be written with sensitivity, respect. courtesy, and consideration.
- Terms which are condescending, judgmental, critical, sexist, discriminatory, derogatory, patronising, and negative should never be used.

Least restrictive practice and self-directed support

These are important components of relevant industry standards such as the National Standards for Mental Health Services (NSMHS), NDIS Practice Standards and the provision of quality support. Where appropriate include details that reflect adherence to these standards. For example:

- Who initiated activities and discussions during the support.
- How was the participant consulted and given a choice.
- If consent was obtained and how.

Proofread before closing

Before closing a file note, it is best practice to proofread the note before closing. This is an opportunity to ensure that:

- all relevant and **only** relevant information has been included.
- the File/Case note is clear and there is correct spelling and grammar.
- that there are no errors in the information.
- any corrections on hard copy documents should have a single line struck through with your initials alongside.

3.0 USING THE FACT® METHOD TO WRITE FILE/CASE NOTES

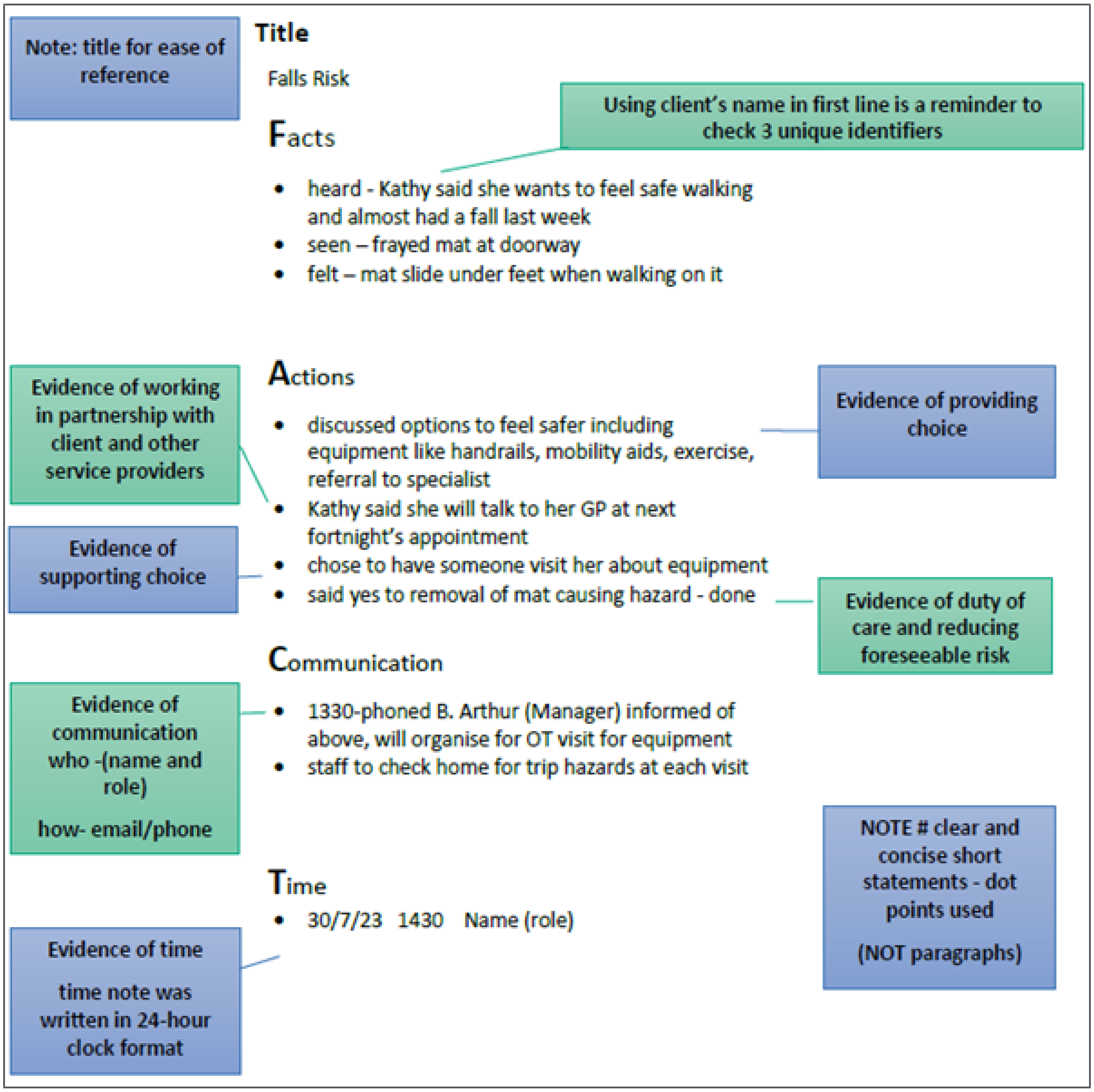
A clear and concise way of writing a note entry is in **dot point format**. Taking dot notes during a shift is an effective way of ensuring that important details of the support are not forgotten and therefore omitted from the File/Case notes.

Date AND Time	• Document date and time in the correct format to avoid misinterpretation.

	• Use 24-hour clock, *e.g. 15.00 instead of 3.00pm.*
Title of the File/Case note	**Tells the reader succinctly what the note is about:** • Incident • Health / Medical • Falls Risk • Behaviour • Phone Call • Email • Shift Summary
F – Facts Information should be **objective** and factual. Write exactly what was said using "quotes".	**What was seen, heard, smelt, or touched:** • **Goals:** What is the client choosing to do or not do? • **Incidents:** Location - what happened, what lead up to the incident, was anyone injured/impacted (if yes, where), who was involved - including any witnesses. • **Complaints:** Heard from person or others and the outcome they would like. • **Risks:** Hazards, health, change in behaviour of person or other, environmental, medication use etc. **Write objectively about what was:** ✓ **Seen:** client hit another client with closed fist / water on kitchen floor. ✓ **Heard:** slurred speech / client said stabbing pain in stomach. ✓ **Smelt:** alcohol / cigarette smoke / odour from wound. ✓ **Touched:** hand hot to touch / skin clammy / stomach hard to touch. ? **Do not use** subjective language, your opinions, thoughts, feelings, or judgements e.g. aggressive, appeared, agitated, confused, **unless** this is followed by a factual / objective description e.g. 'The participant appeared tired; I saw her yawning regularly'. ? Do not add criticism or blame.
A – Actions Were taken to prevent foreseeable harm and were informed by policy/procedure/care and support plan.	**Actions taken by staff, client, family, or others:** • Type of support or prompting provided e.g. verbal prompting, picture card reminder. • Choices or actions taken by the person receiving support. • Information provided e.g. discussion or written information given about choices or consequences. • Care or support plan strategies used. • In response to incidents or complaints e.g. first aid or emotional support.

	- Prevent incident re-occurrence e.g. environmental changes.
C – Communication Communications with relevant stakeholders. Keeping a record of who you have communicated with (their role/position) is important in sharing the risk of legal responsibility.	**Communication by staff, client, family, or others**: - What was communicated by the person, staff, family, or other service providers e.g. outcomes, choices, needs, follow up required. - Who was informed? Give name, role, or organisation. - Who the client wants informed. - How were they informed e.g. email, phone call, text, incident report. - What was communicated e.g. risks, outcomes, client choices, needs. - What was the response (if applicable)? e.g. monitoring, follow-up. - What communication was required by your organisation's procedures/guide.
T- Time/s Support and communication occurred in a timely manner.	**Check time has been included where applicable:** - Date and time the note was written. - The time when important action or communication occurred. - Timeframes for follow-up.
SIGN OFF **Name AND Role**	- Include name – first initial of first name and full surname and role, *e.g. T. Smith, Support Worker.* - Signature on hard copies.

Figure 1: Example Case/File note using the FACT® method (PHI)



Note: title for ease of reference

Title

Falls Risk

Using client's name in first line is a reminder to check 3 unique identifiers

Facts

- heard - Kathy said she wants to feel safe walking and almost had a fall last week
- seen – frayed mat at doorway
- felt – mat slide under feet when walking on it

Evidence of working in partnership with client and other service providers

Evidence of providing choice

Actions

- discussed options to feel safer including equipment like handrails, mobility aids, exercise, referral to specialist
- Kathy said she will talk to her GP at next fortnight's appointment
- chose to have someone visit her about equipment
- said yes to removal of mat causing hazard - done

Evidence of supporting choice

Evidence of duty of care and reducing foreseeable risk

Communication

- 1330-phoned B. Arthur (Manager) informed of above, will organise for OT visit for equipment
- staff to check home for trip hazards at each visit

Evidence of communication who -(name and role)

how- email/phone

Time

- 30/7/23 1430 Name (role)

Evidence of time

time note was written in 24-hour clock format

NOTE # clear and concise short statements - dot points used

(NOT paragraphs)

- **See Appendix 1 (below):** PHI quick reference Guide - FACT® Method Checklist

4.0 TROUBLESHOOTING CASE/FILENOTES

Writing a case note on behalf of someone else	If at any time a person is unable to complete the required File/Case note, and another staff member completes the note, this must be clearly documented identifying the reason: e.g. "I am completing this File/Case note on behalf of B. Jones – Support Worker, he was unable to complete the File/Case notes due to an injury sustained on shift."

Adding a note in the wrong person's file.	If a note is made in the wrong person's Case/File notes rule a line through the entry and make a note that the information was written in the wrong client's file by using the words 'notes entered against incorrect client'.
File Note Correction	Under privacy laws information needs to be accurate, current, and correct. Care should be taken to avoid errors and omissions when entering File/Case notes as they are legal documents. Saved information cannot be deleted. If a new file note to correct an error or omission is required, this should be recorded as *'File Note Correction - Late entry'*. Make a note at the top that this is an edit and refer to the date of the entry that you are editing. In some instances, it is also advisable to provide an explanation for the alteration to avoid the impression that information was purposefully left out. If required, inform the appropriate stakeholders of the alteration or addition.

5.0 RELATED DOCUMENTS

Document Name
Nil

6.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	27 July 2023
Date of Issue	8 August 2023	**Document Number**	i090800_v1_230824

(Uncontrolled when printed)

APPENDIX 1: FACT® Method Checklist Quick Reference Guide

	FACT® Method Checklist	Yes	No
Title and Author	Does the note have a title which tells the reader what the note is about?		

	Is it clear who wrote the note, and their role?		
Facts	Are the words factual and objective? (e.g., what is seen, heard, smelt, or touched)		
	Has the privacy of others been maintained?		
	Is the language simple/easy English?		
	Is the note free from jargon or slang?		
	Is the note free from criticism, judgment, or blame?		
	If used, are subjective words followed by a factual/objective description?		
	Is the note clear and concise (short statements, not paragraphs)?		
	If abbreviations are used, are they in your organisations approved abbreviation list?		
Actions	Is it clear from the note what actions were taken?		
	Is there evidence of person centered/person directed care?		
	Are the actions relevant to the person's care or support plan?		
	Were the writers' actions within their scope of practice?		
	Were actions informed by organisational procedure/guidelines?		
Communication	Does the note include the name and role of who was communicated with?		
	Have responses to communication been included?		
Timeframes	Have the times of important events and communication been included?		
	Have timeframes for follow up or monitoring been included?		
	Does the note show the time and date it was written?		
Quality	Is the note free from irrelevant information? Does the note provide evidence of staff competence?		

1.7.3 Incident Management

1.0 INTRODUCTION / GENERAL

As a registered provider of community supports STEPS Group Australia (STEPS) is required to have an incident management system that records and manages incidents that occur while supports or services are being provided to people with disability.

STEPS is mindful of the critical role it has in providing service and supports to people with disability, their families and carers and understands it has a legal and ethical obligation to ensure the physical and emotional safety of its workers, participants, and those whom we come in to contact with during our daily work activities.

All STEPS workers are responsible for preventing, responding, and reporting incidents using the processes described in this procedure. All incidents that happen in the delivery of registered community supports and services will be recorded and managed in accordance with the minimum requirements. An Easy Read version for Incidents is also available Easy Read Incidents (i090702).

This procedure applies only to NDIS (Community Support, Pathways and Workmates) and Mental Health program participants. All other incidents not related to these programs are to be processed according to the WHS Incident Notification Procedure (i090200).

1.1 DEFINITIONS

Word	Definition
NDIS	**Pathways, Community Support, Work Mates**
Incident	An incident may mean any of the following: • Acts, omissions, events, or circumstances that occur in connection with providing NDIS supports or services to a person with disability and have, or could have, caused harm to the person with disability. • Acts by a person with disability that occur in connection with providing NDIS supports or services to the person with disability and which have caused serious harm, or a risk of serious harm, to another person. • Reportable incidents that have or are alleged to have occurred in connection with providing NDIS supports or services to a person with disability.
Reportable Incidents	Reportable incidents are serious incidents or alleged incidents which result in harm to a NDIS participant and occur in connection with NDIS supports and services. Specific types of reportable incidents include: • The death of a person with disability. • Serious injury of a person with disability (fractures, burns, deep cuts, extensive bruising, head or brain injuries, or any other injury requiring hospitalisation). • Abuse or neglect of a person with disability (physical, psychological, or emotional, financial, systemic abuse). • Unlawful sexual or physical contact with, or assault of, a person with disability (excluding, in the case of unlawful physical assault, contact with, and impact on, the person that is negligible).

	• Sexual misconduct committed against, or in the presence of, a person with disability, including grooming of the person for sexual activity. • The use of a restrictive practice in relation to a person with disability, other than where the use is in accordance with an authorisation (however described) of a State or Territory in relation to the person or a behaviour support plan for the person.
In Connection with the provision of supports or services	This is a broad term that covers incidents that: • may have occurred during the course of supports or services being provided. • arise out of the provision, alteration, or withdrawal of supports or services; and/or • may not have occurred during the provision of supports but are connected because it arose out of the provision of supports or services. • Incidents may occur in a variety of settings including private home of the participant, residential care, supported accommodation, STEPS premises or in the community where STEPS is supporting the participant.
MENTAL HEALTH PROGRAM INCIDENTS	
General Incidents	These include: • Participant Self Harming • Dangerous behaviour in a vehicle • Verbal abuse or aggression • Injury to worker (Report to HSR) • Property damage • Seizure • Threat with a weapon.
Major Incidents	Major Incidents are defined as: • an incident that affects or is likely to affect Service users and service delivery. • an incident that relates to any of the services or Service users and that requires an emergency response including fire, natural disaster, bomb threat, hostage situation, death or serious injury, or threat of death or serious injury, of any person or any criminal activity. • a matter where significant media attention has occurred or is likely to occur. Major Incidents include: o Serious Injury o Assault

	o Fire o Emergency Services attended o Bomb threat o Criminal activity o Death o Explosion o Hostage situation o Natural Disaster o Participant whereabouts unknown o Violation of human rights, abuse, harm, or neglect of a participant o Any incident that may relate to participant subject to interventions by Adult Mental Health staff o Media attention – that has occurred or likely to occur o Witness to an event during a participant visit or in vehicle.

2.0 IDENTIFYING INCIDENTS

Incidents may be identified in several ways, these include:

- where you or another person observes the incident;
- a person with disability makes a disclosure about the incident; or
- another party informs your provider that the incident occurred.

Some incidents will be simple to identify. However, other incidents may be harder to identify, especially where the person involved is afraid to communicate or has limited communication.

All workers have a responsibility and a role to play in preventing major incidents for the safety of participants and work colleagues. Instances where workers identify potential problems regarding either their own safety, the safety of participants or others, should follow the processes in this procedure and on the Incident Report (i090701).

At times there may be indicators or signs displayed by an individual which could indicate potential incidents, especially where they involve abuse, neglect, sexual misconduct, or unauthorised use of restrictive practices.

Refer to the Recognising and Responding to Abuse, Neglect and Exploitation Procedure (i051400) for a table that sets out the potential indicators and signs, where associated with a change in behaviour, may warrant further exploration to understand why the person is responding as they are.

3.0 RECORDING INCIDENTS

Recording and reporting incidents is essential to identify any risk factors related to work practices and to either assist in preventing incidents or alternatively highlight the need for reviewing work practices and procedures.

The Incident Report (i090701) is to be completed if you, or another person observes the incident or where a person with a disability makes a disclosure to you, or if another party informs you of an incident.

If abuse, neglect, or exploitation is suspected or reported use the Reporting Abuse, Neglect and Exploitation Form (i051401). All information must be kept confidential to protect the person's rights and privacy.

4.0 RESPONDING TO INCIDENTS

Workers will respond in a manner that is dignified, respectful and professional to minimise distress of the event.

4.1 WHEN AN INCIDENT OCCURS

- Ensure that all involved are safe and free from danger. If necessary, remove the individual from the immediate area.
- If death or injuries have occurred call the appropriate emergency services immediately.
- For an immediate act of violence or threats of violence call the police immediately.
- Where relevant, maintain the scene of the incident, take photos, and protect any personal articles or evidence involved. You can protect an area by not cleaning where the incident took place. Do not allow anyone to enter until police arrive. You can protect evidence by encouraging the person not to change clothes or bed linen etc.
- Contact your manager, inform them of the situation and follow their direction.
- Complete the Incident Report (i090701).
- Complete the Reporting Abuse, Neglect and Exploitation Form (i051401) if abuse, neglect, or exploitation is suspected or reported.

4.2 WHEN A PARTICIPANT DISCLOSES AN INCIDENT

- Respond calmly and with sensitivity.
- Provide a safe and private environment.
- Explain to the participant that the information they provide will be required to be reported to your manager.
- Acknowledge the participants/students courage for raising their concerns and ensure they feel supported.
- Listen and assess the level of risk to the participant in terms of likelihood of immediate harm or possible harm through the participants relayed account.
- Workers are not to ask probing questions. Questions should consist of:
  - – What happened?
  - o When did it happen?
  - – Where did it happen?

  - Who was involved?

- Open questions may include:
  - "Tell me more about that."
  - "What do you mean by…?"
  - "Can you tell me …?"
  - "What happened next?"

- DO NOT ask these type of questions:
  - "Was it John who did this to you?" (instead ask "Who did this to you?")
  - "Did this happen today" (instead ask "What day did this happen?")
  - "Did this happen in the kitchen?" (instead ask "Where did this happen?").

Workers are not to problem solve or counsel during this period of disclosure. A certified professional aligned to the type of abuse will be sourced to conduct such conversations.

Contact your Team Leader, Manager or Executive Manager, inform them of the situation and follow their direction. Complete the Incident Report (i090701) and/or the Reporting Abuse, Neglect and Exploitation Form (i051401) to record the incident.

5.0 REPORTING INCIDENTS

Workers must adopt emergency measures (i.e., contact applicable emergency services) to ensure the safety of participants, workers, and members of the community.

Workers must verbally report the incident to the Team Leader, Manager or Executive Manager as soon as possible after the incident occurs, then complete and lodge an Incident Report (i090701) as soon as is practicable and within twelve (12) hours of the incident.

The Manager or Executive Manager will notify the Managing Director or Chief Operating Officer (COO) as soon as they become aware that the incident constitutes a Reportable Incident and forward them a copy of the completed Incident Report (i090701). Where applicable and consent is provided, the Manager or Executive Manager will contact the participant's next of kin/formal nominee to advise of the incident.

The Manager or Executive Manager will review any impact to the services we provide and coordinate and implement any actions as required. The potential for disruption to the lives of participants and workers varies according to the severity of the event and the number of people involved. Individuals may be affected according to the closeness of their relationship to those involved and, their own experiences in life and their coping skills.

If a worker has been injured, either the worker or the Manager must refer to the WHS Incident Notification Procedure (i090200). Once informed of the incident, the Work Health and Safety Officer (WHSO) will support the Manager through the process for managing work injuries.

The WHS Incident Notification Procedure (i090200) is also used for participant incidents that are not NDIS or Mental Health program related.

The Manager or Executive Manager will make debriefing available for all those involved or affected by the incident, both directly and indirectly as soon as they are physically able to participate and encourage workers to utilise Employee Assistance Services (EAP) as per the Employee Assistance Program (EAP) Procedure (e230100). Feedback will be provided to all involved in the incident and where appropriate a list of recommended actions for follow up including any ongoing support required by staff and others involved. The COO and/or Managing Director may be called upon to provide support to program management and workers in the event of a Reportable Incident. The Manager or Executive Manager is also to provide a brief background of the incident to counselling personnel.

The Manager or Executive Manager will liaise with the Work Health and Safety Officer / Rehabilitation and Return to Work Coordinator regarding the progress of the person/persons who experienced the Reportable Incident, and for other workers to negotiate their return-to-work strategy.

After one-month continuous return to full duties, the Manager or Executive Manager is to assess the health (absences, well-being, etc.) and the effect on the work performance of the person/persons who experienced the Reportable Incident and take appropriate action where required to assist in full recovery.

The COO and/or Managing Director will notify or delegate the Executive Manager to notify the appropriate authorities such as, but not limited to:

- The Police
- NDIS Commission
- Community Funding Queensland Health
- Office of the State Coroner.

All media enquiries are to be directed to the Managing Director regardless of their nature or circumstances.

6.0 REPORTABLE INCIDENTS

6.1 NDIS REPORTABLE INCIDENTS

If the incident is an alleged or 'Reportable Incident,' STEPS must give details about the incident to the NDIS Quality and Safeguards Commission. Details of certain incidents and allegations (refer to the definition of Reportable Incidents, *NDIS Incident Management & Reportable Incidents Rules 2018*, dot points a to e) require an *Immediate Notification* to be created and submitted via the *NDIS Quality and Safeguards Commission Portal* **within 24 hours** of becoming aware of it, including the five day follow up report. An exception to this timeframe applies to the use of a restrictive practice not in accordance with a required state or territory authorisation and/or not in accordance with a behaviour support plan. In this case, the *NDIS Quality and Safeguards Commission Portal* must be notified within five business days.

The Executive Manager or delegate, Manager – Behavior Support & Complex Client Intervention, is the person authorised and responsible for submissions to the NDIS Quality and Safeguards Commission. The Executive Manager will submit the five-day follow up report via the portal.

In the event that the *NDIS Quality and Safeguards Commission Portal* 'My Reportable Incidents' page cannot be accessed, the Executive Manager will contact the NDIS Commission for support. If this occurs outside business hours, then STEPS should advise the NDIS Quality and Safeguards Commission of these issues as soon as possible via email to reportableincidents@ndiscommission.gov.au

The email must include:

- The steps taken to complete the authorised notification form and the presenting issue.

- The name of the impacted participant.
- Describe the immediate response and steps taken to ensure the impacted participant was safe.
- Brief description of the reportable incident.
- Whether other authorities, such as the police, were notified.

6.2 MHP REPORTABLE INCIDENTS

Workers must adopt emergency measures (i.e., contact ambulance, police, and emergency services) to ensure the safety of participants, workers, and members of the community.

Workers must verbally report the incident to the Team Leader or Manager Mental Health Programs immediately after the incident occurs, then complete and lodge an Incident Report (i090701) as soon as is practicable and within **24 hours** of the incident.

The Team Leader or Manager Mental Health Programs will notify the Executive Manager - Community Support as soon as they become aware of the major incident and forward a copy of the completed Incident Report (i090701).

Where the participant has provided consent, the Manager Mental Health Programs or Executive Manager will contact the participant's family to advise of the incident.

The Team Leader and Manager Mental Health Programs will review any impact to the services we provide and coordinate and implement any actions as required. The potential for disruption to the lives of participants and workers vary according to the severity of the event and the number of people involved. Individuals may be affected according to the closeness of their relationship to those involved and their own experiences in life and their coping skills.

Debriefing will be made available for all those involved or affected as outlined in section 5.0 of this document.

As STEPS is in receipt of Queensland Health funding, the death of a person with a disability who was receiving services partially or fully funded by Queensland Health, at an agency facility or in the person's own home, must be reported to the Coroner as a death in care. The Manager Mental Health Programs or the Executive Manager will notify the Office of the State Coroner and as instructed by the Coroner, the police will also need to be notified of the death in care.

The Manager Mental Health Programs or the Executive Manager will also notify The Senior Director, Community Funding Qld Health (email: communityfunding@health.qld.gov.au).

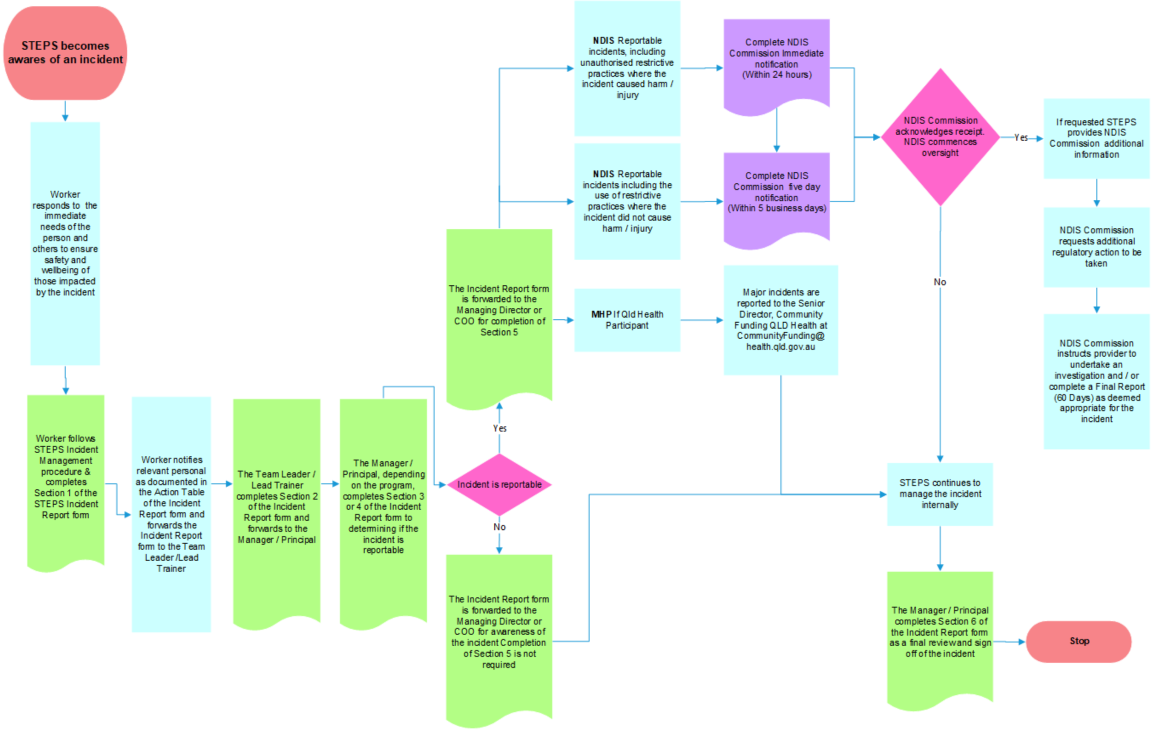
7.0 INCIDENT MANAGEMENT REGISTER

STEPS will use an *Incident Management Register* to record key data which will enable the generation of reports to identify trends and opportunities for continual improvement.

The Team Leader and/or Manager will update the *Incident Management Register* located in 'O' Drive under the relevant program in the 'Reporting' Folder with the required information for each incident. The incident must be recorded in the register within 30 days from the incident date.

8.0 INCIDENT MANAGEMENT MONTHLY REPORTING

Monthly reports will be generated by the Manager, who will 'refresh' the data at the end of each month. This data can be presented at management meetings, team meetings and be included in Board reports.


STEPS becomes awares of an incident
Worker responds to the immediate needs of the person and others to ensure safety and wellbeing of those impacted by the incident
Worker follows STEPS Incident Management procedure & completes Section 1 of the STEPS Incident Report form
Worker notifies relevant personal as documented in the Action Table of the Incident Report form and forwards the Incident Report form to the Team Leader /Lead Trainer
The Team Leader / Lead Trainer completes Section 2 of the Incident Report form and forwards to the Manager / Principal
The Manager / Principal, depending on the program, completes Section 3 or 4 of the Incident Report form to determining if the incident is reportable
Incident is reportable
Yes
No
The Incident Report form is forwarded to the Managing Director or COO for completion of Section 5
The Incident Report form is forwarded to the Managing Director or COO for awareness of the incident Completion of Section 5 is not required
NDIS Reportable incidents, including unauthorised restrictive practices where the incident caused harm / injury
NDIS Reportable incidents including the use of restrictive practices where the incident did not cause harm / injury
MHP If Qld Health Participant
Complete NDIS Commission Immediate notification (Within 24 hours)
Complete NDIS Commission five day notification (Within 5 business days)
Major incidents are reported to the Senior Director, Community Funding QLD Health at CommunityFunding@ health.qld.gov.au
NDIS Commission acknowledges receipt. NDIS commences oversight
Yes
No
If requested STEPS provides NDIS Commission additional information
NDIS Commission requests additional regulatory action to be taken
NDIS Commission instructs provider to undertake an investigation and / or complete a Final Report (60 Days) as deemed appropriate for the incident
STEPS continues to manage the incident internally
The Manager / Principal completes Section 6 of the Incident Report form as a final reviewand sign off of the incident
Stop

i090703_v1_221103

9.0 RELATED DOCUMENTS

Document Name	Document Name
Easy Read Incidents (i090702)	Employee Assistance Program (EAP) Procedure (e230100)
Incident Management Register *Refer to The Quality Assurance & Risk Team*	Incident Report (i090701)
NDIS Commission Portal	Recognising and Responding to Abuse, Neglect and Exploitation Procedure (i051400)
Reporting Abuse, Neglect and Exploitation Form (i051401)	WHS Incident Notification Procedure (i090200)

10.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	29 February 2024

Effective Date	6 March 2024	Document Number	i090700_v3_240306

(Uncontrolled when printed)

1.7.4 Managing and De-Escalating Participants Challenging Behaviours

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to providing assistance and support to employees who encounter participants with challenging and/or aggressive behaviours. STEPS aims to provide a consistent and safe environment for both participants and employees

1.1 DEFINITIONS

Challenging Behaviour - For the purpose of this procedure, challenging behaviour is defined as any incident where an employee or participant is verbally abused, threatened or assaulted in circumstances arising out of, or in the course of, their employment or attendance, where there is a threat of/or actual physical property damage or where there is a disruption.

Within this definition:

- Threat means a statement or behaviour that causes a person to believe they are in danger of being physically attacked. It may involve an actual or implied threat to safety, health, or wellbeing. The threat can also include a statement or behaviour which causes a person to believe that property damage could occur.
- Physical attack means the direct or indirect application of force by a person to the body of, or clothing or equipment worn by another person, where the application of this force creates a risk to health and safety.
- Property damage means the direct or indirect action of the person which results in damage to objects or property which belongs to the person or others.

Neither intent nor ability to carry out the threat is relevant. The key issue is that the behaviour creates a risk to health and safety. Examples can include, but are not limited to:

- Verbal
- Punching
- Biting
- Pushing
- Attack with a weapon
- Sexual Harassment or assault-Physical or psychological abuse

- Scratching
- Grabbing
- Threats
- Throwing objects/furniture
- Any form of indecent physical contact

2.0 WHEN CHALLENGING BEHAVIOURS ARISE

If any person displays challenging behaviours, the employee will need to balance their duty of care to protect other participants and as well as themselves.

It is important to note that the associated risks for challenging behaviours are increased when the person is experiencing psychosis or substance use or dependence. Some types of personality disorders are also associated with increased risk of aggression and violence. Threats of violence often precede violence, take any threats or warnings seriously.

Being aware of any previous history of aggression or violence is a good place to start. In some instances, if the person has a history of challenging behaviour, there may be a documented reactive protocol which provides a strategic response in relation to their challenging behaviour.

What is perceived as aggression can vary between Individuals and across cultures. The person may not be aware that they are being perceived as aggressive. The best way to respond to early signs of or low-medium aggressive behaviours is to take action to de-escalate the situation.

3.0 DE-ESCALATION

De-escalation is avoiding or preventing an escalation in challenging behaviour. Sometimes this is called conflict resolution, verbal de-escalation, or crisis intervention.

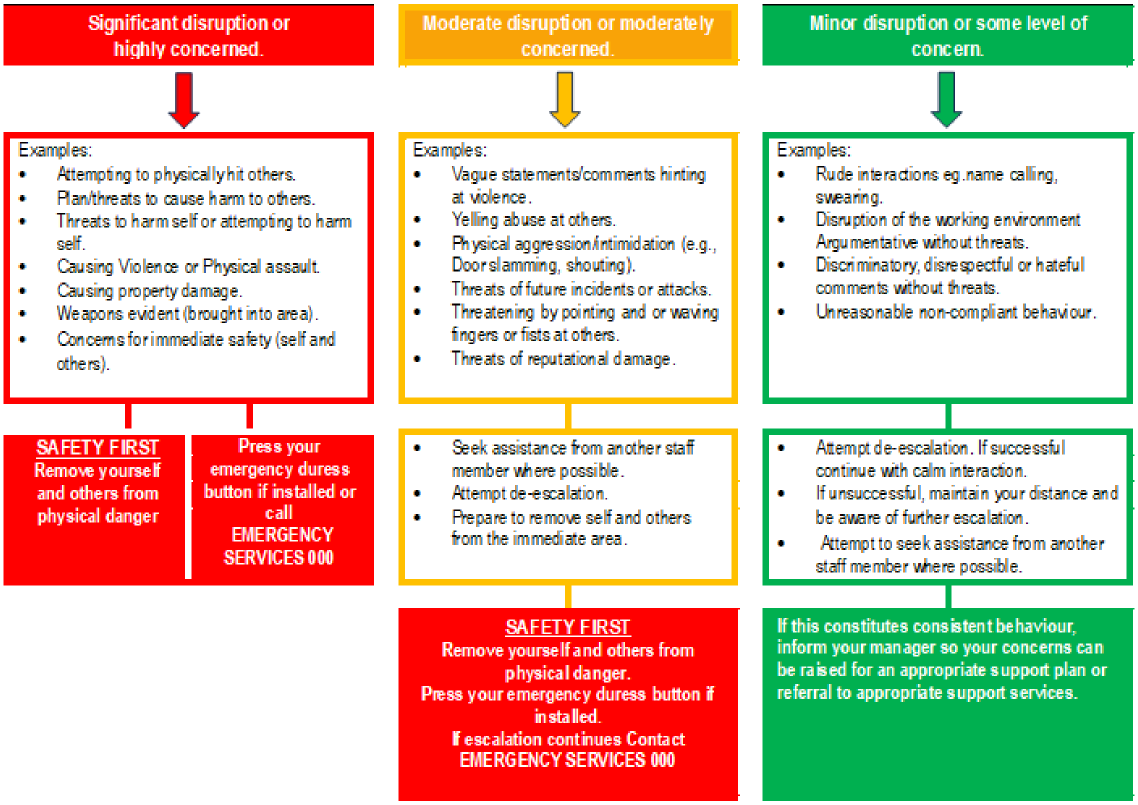
It’s an essential skill for working with others who may display challenging behaviour. Working with people we must be able to display patience, empathy, compassion, and a genuine desire to help people. De-escalation is important because there will be times when we face challenging situations, including people who can display or engage in challenging behaviour.

Here are some tips that everyone should consider when dealing with participants/people who may present with challenging behaviours.

1. Maintain non-threatening body language.
2. Stand back about three feet, ensure you maintain eye contact without staring.
3. Stay calm and professional, your there to help.
4. Focus on solving the immediate problem if it is apparent.
5. Show empathy.
6. Accept slow responses as they may be having difficulty processing.
7. Give simple, clear verbal instructions.
8. Look for the root of the problem and attempt to assist them dealing with the problem.

9. Be flexible, if possible.
10. Give the person time to think about the situation.

No person, group, or set of conditions can guarantee that a situation will proceed constructively. If de-escalation is not working, stop! If the situation feels unsafe, leave and call for help.



Significant disruption or highly concerned.

Examples:
- Attempting to physically hit others.
- Plan/threats to cause harm to others.
- Threats to harm self or attempting to harm self.
- Causing Violence or Physical assault.
- Causing property damage.
- Weapons evident (brought into area).
- Concerns for immediate safety (self and others).

SAFETY FIRST Remove yourself and others from physical danger

Press your emergency duress button if installed or call EMERGENCY SERVICES 000

Moderate disruption or moderately concerned.

Examples:
- Vague statements/comments hinting at violence.
- Yelling abuse at others.
- Physical aggression/intimidation (e.g., Door slamming, shouting).
- Threats of future incidents or attacks.
- Threatening by pointing and or waving fingers or fists at others.
- Threats of reputational damage.

- Seek assistance from another staff member where possible.
- Attempt de-escalation.
- Prepare to remove self and others from the immediate area.

SAFETY FIRST
Remove yourself and others from physical danger.
Press your emergency duress button if installed.
If escalation continues Contact EMERGENCY SERVICES 000

Minor disruption or some level of concern.

Examples:
- Rude interactions eg.name calling, swearing.
- Disruption of the working environment Argumentative without threats.
- Discriminatory, disrespectful or hateful comments without threats.
- Unreasonable non-compliant behaviour.

- Attempt de-escalation. If successful continue with calm interaction.
- If unsuccessful, maintain your distance and be aware of further escalation.
- Attempt to seek assistance from another staff member where possible.

If this constitutes consistent behaviour, inform your manager so your concerns can be raised for an appropriate support plan or referral to appropriate support services.

NOTE: If you feel immediately threatened or have an urgent incident where people's safety is at risk, contact Emergency Services on 000

For staff debriefs, advice on managing future incidents, or training in challenging behaviours, contact your line manager or for individual support the Employee Assistance Program (Converge 1300 687 327)

FOLLOWING ALL INCIDENTS, STAFF MUST COMPLETE AN INCIDENT REPORT AS SOON AS POSSIBLE AND FORWARD TO THEIR LINE MANAGER.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Incident Management (i090700)	Incident Report (i090701)
Employee Assistance Program (EAP) (e230100)	Easy Read Incidents (i090702)

5.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	29 February 2024
Effective Date	6 March 2024	**Document Number**	i051300_v2_240306

(Uncontrolled when printed)

1.7.5 Recognising and Responding to Abuse, Neglect and Exploitation

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to upholding human rights as per the United Nations Declaration of Human Rights, 1948 and maintaining a culture that respects the rights of all customers.

To achieve these goals STEPS maintains policies and procedures that support the prevention of abuse, neglect and exploitation including Code of Conduct and Ethical Behaviour (e210007), Safeguarding Policy (i010115), Safeguarding, Preventing Abuse, Neglect and Exploitation Procedure (i052500), Recruitment and Selection (e200100), Criminal History Checks (e200200), Feedback and Complaints Policy (i010103), Feedback Procedure (i040100), Complaints Procedure (i040500) and Employee Grievance Procedure (e210100).

Customers of STEPS services receive an information booklet on commencement with STEPS outlining what they can expect to receive as a participant of our services and a copy of Feedback and Complaints Policy (i010103) and Privacy Policy (i010106).

1.1 DEFINITIONS

Abuse	The violation of a person's human rights, through an act or actions of commission or omission, by another person, or persons. This includes all forms of physical and mental abuse, exploitation, coercion, or ill-treatment. For example: • physical abuse • emotional abuse • threats of, or actual violence, verbal, emotional or social abuse • sexual harassment, bullying or abuse • sexual criminal offences • cultural or identity abuse, such as racial, sexual or gender-based discrimination or hate crime • coercion and exploitation • abuse of power • neglect.
Neglect	The failure to provide the necessary care, aid or guidance to dependent adults or children by those responsible for their care.

Exploitation	Taking advantage of the vulnerability of a person in order to use them, or their resources, for another's profit or advantage (e.g. Financial abuse).
Reportable Conduct	A *sexual offence*, such as: • sexual touching of a person without consent • a child grooming offence • production, dissemination or possession of child abuse material.
	Sexual misconduct, such as: • descriptions of sexual acts without a legitimate reason to provide the descriptions • sexual comments, conversations or communications • comments to a child, young person or vulnerable person that express a desire to act in a sexual manner towards that person or another person.
	Ill-treatment of a child, young person or vulnerable person, such as: • making excessive or degrading demands of a child, young person or vulnerable person • a pattern of hostile or degrading comments or behaviour towards a child, young person or vulnerable person • using inappropriate forms of behaviour management towards a child, young person or vulnerable person.
	An *assault* against a child, young person or vulnerable person, such as: • hitting, striking, kicking, punching or dragging a child, young person or vulnerable person • threatening to physically harm a child, young person or vulnerable person.

2.0 RECOGNISING ABUSE, NEGLECT AND EXPLOITATION

Abuse, neglect and exploitation can take many forms and while no single behaviour is an absolute indicator it is useful to be aware of signs and indicators to assist in recognising them.

PHYSICAL ABUSE Any non-accidental physical injury or injuries to a child or adult, such as inflicting pain of any sort, or causing bruises, fractures, burns, electric shock, or unpleasant sensation (e.g. taste, heat or cold) as well as restrictive practices which are not contained in the client's positive behaviour support / person centred plan.	
Physical Indicators: • unexplained cuts, abrasions, bruising or swelling	**Behavioural Signs:** • avoidance of particular staff, fear of a particular person • sleep disturbances

<table>
<tr><td>• unexplained burns or scalds, cigarette burns
• rope burns or marks on arms, legs, neck, torso
• unexplained fractures, strains or sprains; dislocation of limbs
• bite marks
• dental injuries
• Ear or eye injuries.</td><td>• changes in behaviour (e.g. unusual mood swings, uncharacteristic aggression)
• changes in daily routine, changes in appetite
• unusual passivity, withdrawal
• self-harm, suicide attempts
• inappropriate explanations of how injuries occurred
• Excessive compliance to staff.</td></tr>
<tr><td colspan="2"><b>SEXUAL ABUSE</b>
Any sexual contact between an adult and a child 16 years of age or under; or any sexual activity with a person with impairment of the mind (as defined under ‘Definitions’ in the Queensland Criminal Code). Sexual activity includes intercourse, genital manipulation, masturbation, voyeurism, sexual harassment, and also inappropriate exposure to pornographic media etc.</td></tr>
<tr><td><b>Physical Indicators:</b>
• direct or indirect disclosure of abuse or assault
• trauma to the breasts, buttocks, lower abdomen or thighs
• difficulty walking or sitting
• pain or itching in genital and/or anal area; bruising, bleeding or discharge
• self-harm, abuse, suicide attempts
• torn, stained or blood-stained underwear or bedclothes
• sexually transmitted diseases, pregnancy
• Unexplained money or gifts.</td><td><b>Behavioural Signs:</b>
• sleep disturbances
• changes in eating patterns
• inappropriate or unusual sexual behaviour or knowledge
• changes in social patterns
• sudden or marked changes in behaviour or temperament
• anxiety attacks, panic attacks, clinical depression
• refusal to attend usual places (e.g. work, school, respite)
• going to bed fully clothed
• Excessive compliance to staff.</td></tr>
<tr><td colspan="2"><b>PSYCHOLOGICAL OR EMOTIONAL ABUSE</b>
Verbal communication that is threatening or demeaning, threats of maltreatment, harassment, humiliation, intimidation, failure to interact with a person or to acknowledge the person’s presence, or denial of cultural or religious needs and preferences.</td></tr>
<tr><td><b>Physical Indicators:</b>
• speech disorders</td><td><b>Behavioural Signs:</b>
• self-harm or self-abusive behaviours
• challenging / extreme behaviours</td></tr>
</table>

• in the case of a child, lags in physical development, failure to thrive • injuries sustained from self-harm or abuse • suicide attempts • Anxiety attacks	• excessive compliance to staff • very low self-esteem, feelings of worthlessness • clinical depression • marked decrease in interpersonal skills • Extreme attention-seeking behaviour.
FINANCIAL ABUSE Refers to the illegal or improper use of a person's property or finances or the withholding of another person's resources by someone with whom the person has a relationship implying trust.	
Physical Indicators: • no access to, or unwarranted restrictions on, personal funds or bank accounts • no records, or incomplete records kept of expenditure and purchases • no inventory kept of significant purchases • person controlling the finances does not have legal authority • misappropriation of money, valuables or property • forced changes to a person's will • persistent failure to produce receipts • Receipts indicating unusual or inappropriate purchases.	**Behavioural Signs:** • person has insufficient money to meet normal expenses • Person is persistently denied outings and activities due to lack of funds.
CHEMICAL ABUSE Refers to any misuse of medications and prescriptions, including the withholding of medication and over-medication.	
Physical Indicators: • Abuse of prescribing rights by staff / over–administration of medication	**Behavioural Signs:** • persistent over–activity • unusual levels of confusion/disorientation
ABUSE THROUGH DENIAL OF ACCESS TO LEGAL REMEDIES Denial of access to justice or legal systems that are available to other citizens and denial of informal or formal advocacy support requested by the client or his/her substitute decision maker.	

<table>
<tr><td><b>Physical Indicators:</b>
• Consistent denial of telephone or internet access.</td><td><b>Behavioural Signs:</b>
• person does not seek privacy to undertake activities normally undertaken in private
• Person indicates they have no-one to speak to about things they are unhappy about.</td></tr>
<tr><td colspan="2"><b>SYSTEMATIC ABUSE</b>
Is the form of abusive conduct on the part of agents that is facilitated by fundamental properties of the system itself, suggesting a predisposition or a susceptibility to abuse that is "built-in" at underlying levels of the system architecture.</td></tr>
<tr><td><b>Physical Indicators:</b>
• no program or inadequate/inappropriate program developed for client
• not endeavouring to use staff of the same gender to perform personal duties for clients
• Providing staff with insufficient training on duty of care and policies and practices related to preventing abuse.</td><td><b>Behavioural Signs:</b>
• person is persistently provided support that does not meet the requirements of their service package
• Person refuses part of their service support due to feeling uncomfortable with particular staff members.</td></tr>
<tr><td colspan="2"><b>NEGLECT</b>
Neglect includes, but is not limited to the following:
• <b>Physical neglect</b> – failure to provide adequate food, shelter, clothing protection, supervision and medical and dental care, or to place persons at undue risk through unsafe environments or practices.
• <b>Passive neglect</b> – the failure to fulfil care-taking responsibilities because of inadequate caregiver knowledge, infirmity, or the failure to implement prescribed services.
• <b>Wilful deprivation</b> – wilfully denying a person access to medication, medical care, shelter, food, a therapeutic device or other physical assistance, thereby exposing that person to risk of physical, mental or emotional harm.
• <b>Emotional neglect</b> – the failure to provide the nurturing or stimulation needed for the social, intellectual and emotional growth or wellbeing of an adult or child.
• <b>Crimes of Omission</b> – negligence, i.e. the failure to act with the appropriate duty of care.</td></tr>
<tr><td><b>Physical Indicators:</b>
• physical wasting, unhealthy weight levels</td><td><b>Behavioural Signs:</b>
• constant tiredness
• persistent hunger</td></tr>
</table>

• poor dental health • food from meals left on face and/or clothes throughout the day • dirty, unwashed body and/or face, body odour • person always wearing the same clothes • ill-fitting and/or unwashed clothes • person is always over- or underdressed for the weather conditions • Food is consistently poor quality, insufficient, inedible and/or unappetising.	• unexpectedly poor social/interpersonal skills • signs of loss of communication and other skills • staff member, service provider, carer or support person consistently fails to bring the person to appointments, events, activities • Person is persistently denied opportunities to socialise with others in the community.
EXPLOITATION Exploitation - is taking advantage of the vulnerability of a person with disability in order to use them, or their resources, for another’s profit or advantage (e.g. Financial abuse).	

3.0 RESPONDING AND REPORTING

All employees and volunteers who witness or are notified (i.e. a disclosure is made) about an incident or allegation of abuse, neglect and exploitation must follow these procedures for responding and reporting abuse.

Anyone raising concerns about abuse, neglect or exploitation are to be supported and, where necessary protected.

All complaints and allegations by a customer, family or carer are to be reported to the relevant manager.

Employees are to take complaints or disclosure of abuse, neglect or exploitation seriously and respond in accordance to STEPS procedures.

3.1 REPORTING PROCESS

Incident Type	Reporting (phone/in person)	Managers to be Notified	Escalation Timeline	Notification Process
Witnessing an incident	If cannot be moved from danger, or person is injured call emergency services.	General Manager Executive Manager - HR CEO and Managing Director	Immediately	Line/Geographic Manager will attend the site immediately and secure the area to protect evidence.

	Advise Line/Geographic Manager			Line/Geographic Manager will inform and update CEO and MD of incident, outcomes and referrals.
Disclosure about an incident	Record the information given by the person. Advise Line/Geographic Manager	General Manager CEO and Managing Director	Within 4 hours	Complete Abuse, Neglect and Exploitation form. Advise General Manager and discuss actions. General Manager will inform and update CEO and MD of incident, outcomes and referrals.
Reportable Conduct (such as a sexual offence, sexual misconduct or ill-treatment of assault of a child)	If cannot be moved from danger, or person is injured call emergency services. Advise Line/Geographic Manager	Executive Manager – HR General Manager CEO and Managing Director	Immediately	Executive Manager – HR to advise on mandatory reporting requirements. Advise General Manager and discuss actions. General Manager will inform and update CEO and MD of incident, outcomes and referrals.
Suspected Abuse	Verbally report to Line/Geographic Manager Escalate if there is no response.	General Manager CEO Managing Director Board Member External body	As soon as possible.	General Manager to document and consider all information to assess risk and advise CEO to agree on future action. CEO to keep MD informed.

All suspected, perceived, potential or actual incidents must be reported.	Verbally report to Line/Geographic Manager. Record in the relevant incident management system.	Line/Geographic Manager General Manager CEO Managing Director	Immediately	Monthly Board Reports

3.2 SUSPECTED ABUSIVE ACTIVITY

Employees, volunteers, contractors and third parties who have grounds to suspect abusive activity must report where there is any suspicion that an incident:

- has taken place
- may take place
- could take place.

This report can be made, or escalated through:

a) any member of the board (including the Managing Director);

b) the Chief Executive Officer

c) any manager or supervisor

d) the relevant incident management system.

3.3 INCIDENT

- Ensure that all involved are safe and free from danger. If necessary remove the individual from the immediate area.
- If death or injuries have occurred call the appropriate emergency services immediately.
- For an immediate act of violence call the police immediately.
- Where relevant, maintain the scene of the incident (do not touch anything), take photos and protect any personal articles involved.
- Contact you manager, inform them of the situation and follow their direction.
- Complete the Reporting Abuse, Neglect and Exploitation Form (i051401). All information must be kept confidential to protect people's rights and privacy.

3.4 DISCLOSURE

- Respond calmly and with sensitivity
- Provide a safe and private environment
- Explain to the individual that the information they provide will be required to be reported to your manager

- Acknowledge the persons courage for raising their concerns and ensure they feel supported
- Listen and assess the level of risk to the individual in terms of likelihood of immediate harm or possible harm through the individual's relayed account
- Employees are not to ask probing questions. Questions should consist of:
    - What happened?
    - When did it happen?
    - Where did it happen?
    - Who was involved?
    - How did they know the person present?
- Employees are not to problem solve or counsel during this period of disclosure. A certified professional aligned to the type of abuse will be sourced to conduct such conversations.
- Contact you manager, inform them of the situation and follow their direction.
- Complete the Reporting Abuse, Neglect and Exploitation Form (i051401). All information must be kept confidential to protect people's rights and privacy.

3.5 MANAGER/SUPERVISOR

The relevant manager is responsible for informing the General Manager and escalating as needed to :

- Evaluate the level of risk to the individual and determine:
    - Mandatory reporting requirements to police
    - Reporting requirements to relevant Government service authorities
    - Whether an internal investigation is to be conducted
    - An appropriate service to refer the incident to if applicable
    - If it is believed that the person is at risk of immediate harm or the victim of a criminal offence, the relevant authorities must be contact, including the police.
- Provide support to the employee who managed the incident, this may include counselling and/or debriefing services such as the Employee Assistance Program (EAP)
- Initiate a response to the incident working with the customer, their family or carer towards a resolution
- Advise the Chief Executive Officer, and in consultation:
    - Delegate an appropriate person to work with the customer, their family or carer to self-determine strategies to prevent further incidents of abuse, neglect or exploitation
    - Ensure a formal investigation is conducted and identifying a suitable person to complete the investigation. The CEO will conduct an internal investigation, if it will not conflict with any proceedings of the authorities; all employees, volunteers and contractors must cooperate fully. Every effort will be made to keep such an investigation confidential

- Suspend an employee from work if they are under investigation (internally or by the police) for committing abuse, neglect and exploitation
- Terminate the employment of an employee and ceasing all involvement of a volunteer with the organisation if found guilty of committing abuse, neglect or exploitation (either by an internal investigation or by a court).

All suspected, perceived, potential or actual incidents must be reported and recorded in the relevant incident management system.

4.0 TRAINING AND AWARENESS

STEPS will provide training and education to existing and new employees, volunteers and contractors whose services are regularly engaged in the content and application of this procedure as well as the reporting requirements.

Refresher training will be conducted annually unless changes or amendments either internally or legislatively are introduced prior to the scheduled review date. In addition to training, STEPS Zero Tolerance Poster (i052501) will be displayed in all STEPS site locations.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Code of Conduct and Ethical Behaviour (e210007)	Complaints Procedure (i040500)
Criminal History Checks (e200200)	Employee Grievance Procedure (e210100)
Feedback and Complaints Policy (i010103)	Feedback Procedure (i040100)
Privacy Policy (i010106)	Reporting Abuse, Neglect and Exploitation Form (i051401)
Safeguarding Policy (i010115)	Safeguarding, Preventing Abuse, Neglect and Exploitation Procedure (i052500)
STEPS Zero Tolerance Poster (i052501)	

6.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	24 August 2023
Effective Date	28 August 2023	**Document Number**	i051400_v4_230823

(Uncontrolled when printed)

1.7.6 Safeguarding, Preventing Abuse, Neglect and Exploitation

1.0 INTRODUCTION

STEPS is committed to protecting the welfare and human rights of people that interact with or are affected by our work – particularly those who may be at risk of abuse, neglect, or exploitation.

All people, regardless of their age, gender, race, religious beliefs, disability, sexual orientation, or family or social background, have equal rights to protection from abuse, neglect, and exploitation.

STEPS will promote and protect the interests and safety of children, young adults, vulnerable people and people and risk. We have a zero tolerance for any form of physical and/or sexual abuse.

All employees, volunteers, contractors and third parties of STEPS share responsibility for protecting everyone from abuse, neglect, or exploitation.

1.1 DEFINITIONS

Safeguarding	Protecting the welfare and human rights of people that are, in some way, connected with your organisation, its work – particularly people that may be at risk of abuse, neglect or exploitation.
Child or young person	A person under the age of 18 years.
Vulnerable person	A child or an individual aged 18 years and above who is or may be unable to take care of themselves or is unable to protect themselves against harm or exploitation by reason of age, illness, trauma or disability, or any other reason.
Person at risk	Person aged 18 years and over who: Has care and support needs. Is being abused or neglected, or are at risk of abuse or neglect, and Is unable to protect themselves from abuse or neglect because of their care and support needs.

2.0 RESPONSBILITIES

2.1 BOARD

Protecting all people that interact with or are affected by STEPS Group of Companies.

Responsible for the detection and prevention of abuse to child, young person, or vulnerable persons.

Responsible for ensuring appropriate Safeguarding governance, policies and procedures are in place.

Responsible for ensuring that appropriate and effective internal control systems are in place.

Ensuring that STEPS observes all relevant laws and regulations relating to Safeguarding.

2.2 CHIEF EXECUTIVE OFFICER

Manage and investigate reports of abuse.

Ensure that all staff, volunteers, and contractors are aware of relevant laws, organisational policies and procedures, and the organisation's Code of Conduct and Ethical Behaviour (e210007). Ensure that all the organisation staff, volunteers and contractors are aware of their obligation to report suspected abuse of a child, young person, or vulnerable person in accordance with these policies and procedures.

Ensure the organisation has effective and appropriate ways to manage safeguarding and legal compliance.

Ensure that reports to external parties are made where required.

2.3 EXECUTIVES AND MANAGERS

Promote a culture of safety for children, young persons, and vulnerable people.

Implement this procedure in their area of responsibility.

Assess the risk of abuse to children, young persons and vulnerable people within their area and ensure controls are in place to prevent, detect and respond to incidents.

Facilitate the reporting of any suspected abuse, neglect, or exploitation.

Ensure that there is appropriate safeguarding training in place for staff.

2.4 EMPLOYEES, VOLUNTEERS AND CONTRACTORS

All workers and contractors are responsible for:

- Providing an environment that is safe and supportive of all children, young persons, and vulnerable people's emotional and physical safety.
- Familiarising themselves with STEPS' Safeguarding Policy (i010115) and related procedures; the Code of Conduct and Ethical Behaviour (e210007) and relevant laws in relation to Safeguarding protection.
- Reporting any reasonable belief or incident that a child, young person or vulnerable person safety or welfare is at risk to responsible persons in the organisation or authorities (such as the police and/or the child protection service).
- Fulfilling their obligations as mandatory reporters.

3.0 PREVENTING ABUSE, NEGLECT AND EXPLOITATION

3.1 RECRUITMENT AND SELECTION

STEPS is committed to safe employment and recruitment practices that reduces the risk of harm to children, young adults and vulnerable people from people who are unsuitable to work with them or have contact with them.

All employees, volunteers and contractors will be required to satisfy relevant pre-employment screening prior to commencing their engagement with STEPS. These employment screening requirements will be maintained during employment with STEPS.

3.2 TRAINING AND AWARENESS

STEPS will ensure an appropriate level of safeguarding training is available to its employees, volunteers and contractors and any relevant persons linked to the organisation who requires it.

All employees, volunteers and contractors must undertake mandatory Safeguarding training as part of their induction.

All employees and volunteers working with children, young adults, or vulnerable people, will have awareness that enables them to:

- Understand abuse
- Recognise the abuse, neglect or exploitation ad behaviors of concern, poor practice, and opportunities for improvement
- Process for responding and reporting disclosures, incidents, or potential incidents.

3.3 MANAGING SAFEGUARDING RISKS

STEPS will ensure that safety of children, young people and vulnerable people is part of its overall risk management process.

STEPS will manage the risks of Safeguarding by:

- Having up-to-date risk assessment/s,
- Maintaining a register of legal obligations legislation in all jurisdictions in which STEPS operates.
- Implementing policies, procedures and systems that introduce controls to reduce the likelihood and consequences of incidents.
- Maintaining reporting processes and incident responses.
- Monitoring and reviewing the effectiveness of the safeguarding practices.
- Displaying STEPS Zero Tolerance Poster (i052501) in all STEPS site locations.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Code of Conduct and Ethical Behaviour (e210007)	Safeguarding Policy (i010115)
STEPS Zero Tolerance Poster (i052501)	

5.0 GOVERNANCE

Document Owner	Managing Director	Approval Date	24 August 2023
Effective Date	28 August 2023	Document Number	i052500_v2_230828

(Uncontrolled when printed)

1.7.7 Service Agreement Management

1.0 INTRODUCTION

Service agreements help to ensure participants have an agreed set of expectations of what supports will be delivered and how they will be delivered. A service agreement sets out the responsibilities and obligations for both parties and how to solve any problems should they arise.

2.0 SERVICE AGREEMENTS

All participants require an individually completed service agreement with reference to a person's NDIS plan. An Easy Read document outlining the Service Agreement process is also available, Easy Read Participant Handbook. A service agreement should include:

- A description of the supports that will be provided.
- The cost of those supports.
- How, when and where the participant requires the supports to be delivered.
- How long the participant requires the supports to be provided.
- When and how the service agreement will be reviewed.
- How STEPS will deal with any concerns or questions that may arise and how the participant will be included in this process.
- What the participants responsibilities are under the service agreement – for example, how much notice the participant must give if they cannot attend an appointment.
- What STEPS' responsibilities are under the service agreement – for example, to work with the participant to provide supports that suit their needs.
- What notice is required if STEPS or the participant need to change or end the service agreement and how this is done – for example, by email or mail.

2.1 NEW SERVICE AGREEMENTS

A meeting will be scheduled with the participant and if the participant consents, their family and/or substitute decision maker, to create a service agreement to:

- Establish the expectations.
- Explain the supports to be delivered.
- Explain any conditions attached to the provision of those supports and why those conditions are attached.

It's important that each participant is supported to understand their service agreement and conditions using the language, mode of communication and terms that the participant is most likely to understand.

If the service agreement is written, have the participant and/or authorised substitute decision maker sign it, provide the participant a copy and file the other copy in the participant's record.

Where this is not practicable, or the participant chooses not to have an agreement, record this and note the circumstances under which the participant did not receive a copy of their agreement.

Please be advised that any support or service requested by the participant or their nominee undertaken by STEPS Group will be charged accordingly, regardless of a returned signed agreement.

If a Participant wishes to add a one-off support shift, or would like to make a permanent increase in their support hours, the Community Coordinator or Team Leader can raise an internal request for a Service Agreement using “Request for Service Agreement ”.

Any changes to existing rosters must be sent to the Customer Care Team using “Request for Service Agreement ”.

The Community Coordinator or Team Leader must communicate to the Participant that any additional support shifts can commence no earlier than 2 weeks after the Participant has signed the Service Agreement.

2.2 CHANGING A SERVICE AGREEMENT

A service agreement that has commenced may only be changed if the changes are agreed in writing, signed and dated. Changes can take effect no earlier than 2 weeks after the new Service Agreement has been signed by the Participant.

2.3 SPECIALIST DISABILITY ACCOMMODATION

If supported independent living supports are provided to participants in specialist disability accommodation, arrangements must be clearly documented on roles and responsibilities in a service agreement including:

- How a participant’s concerns about the dwelling will be communicated and addressed.
- How potential conflicts involving participants will be managed.
- How changes to participants circumstances and/or support needs will be agreed and communicated.
- In shared living, how vacancies will be filled, including each participant’s right to have their needs, preferences and situation considered.
- How behaviours of concern, which may put tenancies at risk, will be managed if this is a relevant issue for the participant.

2.4 CANCELLATIONS OR NO SHOWS

A service agreement that has commenced may only be changed if the changes are agreed to by all parties in writing and signed and dated.

Where STEPS receive a short notice cancellation (or no show), STEPS may recover 100% of the fee associated with the activity.

A cancellation is a short notice cancellation (or no show) if the participant has given:

- Less than two (2) clear business days' notice for the support and STEPS are unable to redirect the support worker to another shift.

There is no limit on the number of short notice cancellations (or no shows) that STEPS can claim in relation the participant.

2.5 WHAT IS A 'BREACH OF SERVICE AGREEMENT'?

If STEPS or the participant and/or the participant's representative:

- Fail to do what is required of them under the Service Agreement or Service Agreement.
- Are unable to communicate effectively, resulting in communication breakdown between the parties.
- Ignore workplace health and safety considerations.
- Fail to comply with STEPS' policies and procedures.

2.6 PAYMENT FOR SERVICES AND SUPPORT DELIVERED

Notwithstanding anything in this Service Agreement to the contrary if the Participant:

- Refuses to pay.
- Changes their provider.
- Has no funds available to make the payment.
- Their funding has expired.

STEPS shall have the right to consider it a 'Breach of Service Agreement' and can cancel, suspend or reduce the supports without liability.

The Participant shall be liable for any amount not paid and reasonable costs of collection incurred by STEPS.

2.7 WITHDRAWING A SERVICE AGREEMENT

STEPS service agreements include a required notification period in the event that a support or service is withdrawn or terminated. This notification period is thirty (30) days prior to the delivery of support or service.

2.8 CEASING A SERVICE AGREEMENT

If STEPS decide to cease a commenced Service Agreement or Service Agreement, a minimum of thirty (30) days' notice will be provided. If a participant wishes to end a commenced Service Agreement or Service Agreement, they will need to provide a minimum of thirty (30) days' notice. The thirty (30) days' notice can be waived if STEPS or the participant seriously breaches the Service Agreement.

3.0 NDIS PRICE GUIDE

STEPS is a registered provider under the NDIS and will adhere to the NDIS Pricing Arrangements & Price Limits (Guide). The Guide is a summary of NDIS price limits and associated arrangements (price controls) that apply. The NDIA sets price controls for certain NDIS supports to ensure NDIS participant obtain reasonable value from their support packages. This price guide determines the amount of funding our participants are able to access for these supports and services. History shows these rates increase minimally and in line with CPI. The NDIS Pricing Arrangements & Price Limits is generally issued in the first week of July each year. Cancellation fees are only chargeable if specifically mentioned in the NDIS Pricing Arrangements & Price Limits for that support.

4.0 AMENDMENTS TO RATES

Unless otherwise notified, STEPS will charge the full fee rates applicable to the supports listed in the NDIS Pricing Arrangements & Price Limits for Service Providers, current at the time the supports were delivered ("Price Guide") including, if applicable, the Temporary Transitional Payment rate. STEPS will automatically change and/or increase fee rates when the current Price Guide is amended. Changes in fee rates will be advised to the participant.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Easy Read Participant Handbook (r4000120)	*NDIS Plan*
NDIS Pricing Arrangements & Price Limits (3110015)	NDIS Service Agreement (3110016)
Request for Service Agreement (i100301)	Service Agreement (5000030)

i100300_v2_241104

1.7.8 Suicidal Ideation

1.0 INTRODUCTION / GENERAL

The intention of this procedure is to provide guidelines to workers as to how they should proceed if they are concerned that a client is at risk of suicide or if a client expresses that they are experiencing suicidal ideation. This procedure applies to all employees of STEPS.

1.1 DEFINITIONS

Duty of Care	A Duty of Care exists when someone's actions could reasonably be expected to affect other people. Duty of Care as a concept is part of the larger legal concept of negligence.
Likelihood	In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
Risk	The possibility that harm (death, injury or illness) might occur when exposed to a hazard.
Risk Assessment	Overall process of risk identification, analysis and risk evaluation against benchmarks or standards
Suicide	The intentional taking of one's own life.
Suicidal Ideation	Thinking about, considering or planning suicide; or wanting to take your own life.

2.0 DETECTION

How to detect if a client may be at risk of suicide.

Risk factors increase the likelihood of suicidal behaviour, whereas protective factors reduce the likelihood of suicidal behaviour and work to improve a person's ability to cope with difficult circumstances. Workers need to have a good understanding of both the risk and the protective factors of suicide to assist them in being able to identify clients who are at risk, below are tables of some of the most common risks and protective factors.

It is, however, important to stress that the presence of many or all factors does not necessarily mean that a person is suicidal. It is equally important to assess protective factors and their role in reducing the risk of suicidal behaviours in some individuals.

RISK FACTORS OF SUICIDE

Risk factors are various elements which may increase the likelihood of suicidal ideation and/or tendencies in individuals.

- Previous suicidal
- Guilt and shame
- Mental illness or disorder

behaviour

- Gender (male)
- Unemployment, economic insecurity
- Chronic pain or illness
- Immobility
- Alcohol or other substance abuse
- Low self esteem
- Low sense of control over life circumstances
- Peer rejection
- Hopelessness
- Social isolation
- Family dispute, conflict and dysfunction
- Separation
- Bereavement
- Lack of meaning and purpose in life
- Imprisonment
- Family history of suicide or mental illness
- Poor communication skills
- Abuse and violence
- Financial stress
- Neighbourhood violence and crime
- Poverty
- School failure
- Social or cultural discrimination
- Homelessness
- Exposure to environmental stressors
- Lack of support services
- Geographical isolation

PROTECTIVE FACTORS OF SUICIDE

Protective factors are various elements which may decrease the likelihood of suicidal ideation and/or tendencies in individuals.

- Good mental health and wellbeing
- Gender (female)
- Good physical health
- Absence of alcohol and other drug problems
- Positive sense of self
- Good communication skills
- Sense of meaning and purpose of life
- Physical and emotional security
- Family harmony
- Supportive and caring family
- Supportive social relationships
- Sense of social connection
- Sense of self determination
- Sense of control over life's circumstances
- Safe and secure living environment
- Financial security
- Employment
- Positive educational experience
- Safe and affordable housing
- Equitable community
- Little exposure to environmental stressors

- No family history of suicide or of life
- Good coping skills
- Sense of control over life’s circumstances
- Little exposure to environmental stressors

WARNING SIGNS OF SUICIDE

Most individuals experiencing suicidal ideation give warning signs or signals of their intentions. The best way to prevent suicide is to recognise the warning signs and then know how to respond if you spot them.

- Talking about suicide
- Prior suicide attempt/s
- Finalising affairs e.g. organising a will
- Ceasing activities that use to be important
- Uncharacteristic or impaired judgement or behaviour (e.g. risk taking)
- Physical apathy
- Making a suicide plan
- Sense of hopelessness
- Feeling trapped – like there is no way out
- Giving away valued possessions
- Loss of interest in personal hygiene or appearance
- Loss of interest in sex
- Self-harming behaviour
- Unexplained crying
- Withdrawal from friends, family or society
- Increased alcohol and/or drug use
- Sudden and/or extreme changes in eating patterns
- Increase in minor illnesses

3.0 SAFETY AND DUTY OF CARE

Steps to take if you are concerned that a client may be experiencing suicidal ideation.

SITUATION SENSITIVITY

Take the client and the situation seriously.

It is unfortunately a common myth that ‘people who talk about completing suicide are just attention seeking and probably will not act on it’. Every instance where a client clearly states, or even indirectly implies thoughts of suicide (e.g. joking about death or ambiguous comments such as ‘I won’t be here much longer’, etc.) must be taken seriously.

SUICIDE RISK ASSESSMENT

Complete a suicide risk assessment.

When conducting a suicide risk assessment it is important to take a holistic approach to the assessment, this includes taking into account warning signs, risk factors and protective factors. There is no single risk assessment method that is appropriate for all situations involving suicide and the following information therefore constitutes a guide for best practice. The worker must use their professional judgement on a case by case basis to determine the level of risk.

VERBAL ASSESSMENT

Use questions to support the assessment of a risk.

Discussions to support the assessment of a risk are to be held in a conversational manner with the client. Workers are to incorporate open-ended questioning and active listening skills to explore:

- What is happening for the client?
- Why they are considering the option of suicide?
- What specifically they are considering?
- When they are considering doing it?

3.1 INTENT

Is the client having thoughts of suicide?

If yes, workers need to have a discussion regarding the client's intent. This may include further questioning around:

- How frequently these thoughts are occurring?

  (e.g. hourly, daily, monthly etc.)
- How long the thoughts are lasting?

  (e.g. are they fleeting thoughts that pop in and out of the client's mind or is the client focused on the thoughts for long periods of time?)
- How distressing the thoughts are for the client?

  (e.g. does the client report that they just push the thought out of their mind because they know they will never act on it or are they becoming anxious and/or depressed by the constant thoughts?)
- When did they start to feel this way?

  (e.g. have they been feeling like this for weeks?)

If the client expresses suicidal intent, then the risk assessment must continue.

3.2 WHY

What is currently happening for the client?

Workers are to spend time with the client exploring what is currently happening for the client.

- Was there a single triggering event that has led to the suicidal thoughts or is it more the compounding effect of numerous recent stressors?
- Has there been any recent loss for the client?
- Does the client feel like they have no hope?

Workers should never assume that they know what is happening for the client.

3.3 PLAN

Do they have a plan?

If yes, workers need to continue the discussion to obtain as much details as possible. Areas to cover include:

- **Lethality**
- **Access**

  Does the client have access to the means to carry out the plan, or can they obtain them?
- **Immediacy**

  When does the client plan on acting on the plan?

  (e.g. tonight, or in six months)
- **Location**

  Where is the client planning on carrying out the act?
- **History**

  Is there anything in the client's history that could increase the risk of suicide?

CLIENT RISK FACTORS

Discussion can occur around a variety of risk factors (refer to 2.2 above). Some of these will already be known to workers (e.g. if the client has a mental health diagnosis), however other questions can be asked to ascertain history that the worker is unaware of. Examples of topics to explore include:

3.4 PREVIOUS SUICIDE ATTEMPTS

Has the client ever attempted suicide in the past? If yes, explore the details, such as:

- How long ago did it occur?
- What was the method used?

- Did the client ask for help or did someone find them?
- How does the client feel about the previous attempt now?

3.5 BEREAVEMENT

Has anyone close to them ever died by suicide? Is the client currently experiencing grief around the death of someone close? If yes, explore the details.

3.6 ALCOHOL OR SUBSTANCE MISUSE

Does the client currently, or have they in the past, misused substances? If yes, explore the details.

3.7 SUPPORTS

What does the client's current support structure look like?

Clients with a minimal number of supports may be at higher risk of suicide so it is imperative to talk to the client to understand who they see as valuable supports. This may include but is not limited to:

- Family
- Friends
- Other Residents
- Support Services.

It is important that workers do not make assumptions about the support a client has (e.g. a support worker is a support) as this may not be the way the client views their support network.

RISK LEVEL

Using the information gained from the verbal assessment, and using professional judgement, workers will determine the level of risk for the client. A brief definition of the levels of risk is below, however, workers are reminded that many factors are used to determine overall risk level and the following is just a guide.

No Current Risk	Low Risk	Moderate Risk	High Risk	Severe/Emergency
The client does not currently have suicidal thoughts.	The client is having some suicidal thoughts but has no plan and says that they will not attempt to complete suicide.	The client has suicidal thoughts and has a vague plan which may not be very lethal and says that they will not attempt to complete suicide.	The client has suicidal thoughts and a specific plan that is lethal and says they will not attempt to complete suicide.	The client has suicidal thoughts and a specific plan that is lethal and imminent. They say that they will complete suicide.

4.0 SAFETY AND DUTY OF CARE

STEPS to take to ensure safety, depending on the identified risk of the client.

The following steps may not be relevant for every situation. Workers need to ensure they choose the most appropriate interventions depending on the situation.

LOW / MODERATE / HIGH RISK

4.1 CRISIS SAFTY PLAN

Make a crisis safety plan with the client.

Ask the client "what can you do to keep yourself safe?" It is important that this is the client's plan and is not forced by the worker. What the plan involves will depend entirely on the client. Ideas for things to introduce the client to as possible inclusions in the crisis safety plan include:

- Who the client can call for help

  (e.g. Adult Mental Health, friends, family, support services etc.)

- Strategies that have worked in the past to help alleviate distress

  (e.g. practicing mindfulness, going for a walk, cooking, etc.)

- Reminders of protective factors

  (e.g. photos of children, family, friends, pets etc.)

- Reminders of things coming up to look forward to

  (e.g. holidays, a friend's wedding etc.)

- Anything that may contribute to keeping the person safe

It is preferable to have the plan written so the client can refer back to it as needed and it should be stored in a location of the client's choosing (e.g. fridge, wallet, diary etc.). The worker should seek permission to obtain a copy of the plan to be kept in the client's file to assist with the ongoing consistency of support.

4.2 IDENTIFIED MEANS REMOVAL

Remove any identified means.

It is preferable to get the client to dispose of the identified means (e.g. take medication to the pharmacy, throw razors away, remove all sharp objects from the house etc.), however the worker may be required to remove the means. This is only done if it is safe for the worker to do so and cannot be done against the client's will.

4.3 CLIENT SUPPORT

Ask the client how they would like us to support them.

This seems simple but is often overlooked. This can be the negotiated with the client around program guidelines. For example, a client might request additional support hours, or the worker might be asked to go to the General Practitioner (GP) with them.

4.4 VERBAL SAFETY CONTRACT

Obtain a verbal safety contract.

Through the conversation with the client the worker is to obtain a verbal guarantee that the client will not harm themselves. Sometimes the client will automatically offer this (e.g. “there is no way I would ever act on my thoughts”), however at other times the worker needs to directly ask the client and may even need to put a time frame on the verbal safety contract (e.g. “can you guarantee your safety until you go to your GP on Monday?”).

4.5 IDENTIFIED MEANS REMOVAL

Remove any identified means.

It is preferable to get the client to dispose of the identified means (e.g. take medication to the pharmacy, throw razors away, remove all sharp objects from the house etc.), however the worker may be required to remove the means. This is only done if it is safe for the worker to do so and can be done against the client’s will to ensure their safety.

4.6 CALL 000

Call an ambulance.

It is best to get the client to call an ambulance themselves, however if they refuse or are unable to, then workers are to make the call.

4.7 NOTIFY MANAGER/S

Notify direct line manager/s as soon as practical.

This could be any member of the Executive Leadership Team (ELT) if your direct line manager/s is not available at the time. If it is after hours, then on call should be contacted.

4.8 RELEVANT STAKEHOLDER NOTIFICATION

If applicable in the circumstances, notify Adult Mental Health (AMH) or any other relevant stakeholders. It is again best to have the client do this, however, if they refuse or are unable, workers are to make the call.

IMPORTANT NOTE: If the client’s AMH case manager is not available (e.g. on the weekend or if they are on leave) workers are to say that they need to speak to someone about the client because of suicide concerns. The person taking the call will be able to put the worker onto the most relevant person (e.g. the after-hours worker, the stand in case manager or the team leader).

4.9 SUPPORT CLIENT

Stay with the client.

Workers are to stay with the client until help arrives (e.g. ambulance or mental health assessment team).

4.10 CLARIFICATION

If workers are unsure how to proceed, they are to call their direct like manager/s for assistance and direction.

4.11 ENGAGEMENT

Workers are reminded that any client under the influence of alcohol and/or other drugs cannot make informed decisions. This is particularly relevant for a client that may be under the influence but engages in a safety plan or provides a verbal contract to guarantee safety. This cannot be relied upon.

4.12 MITIGATION

If a client is under the influence, then workers should support them to decrease their level of intoxication (e.g. water, food, time while ensuring safety etc.) before commencing a crisis safety plan or trying to obtain a verbal contact.

4.13 CRISIS SITUATION REPONSE

If the worker believes that a client is at risk while being intoxicated, the Severe/Emergency process detailed above must be implemented.

BORDERLINE PERSONALITY DISORDER (BPD)

The assessment of a suicide risk for a client that has a diagnosis of BPD is complicated as the presence of suicidal and self-harm behaviours is commonly seen as a feature of the disorder. It is therefore imperative that workers supporting clients diagnosed with BPD are familiar with the ongoing case plan for the client around the management of their suicidal ideation and/or behaviour.

ALCOHOL AND/OR OTHER DRUG INFLUENCE

Clients under the influence of alcohol and/or other drugs.

5.0 ONGOING SUPPORT

Ongoing support for the client.

All workers are responsible for communicating any concerns of risk or incidents that have occurred to the client’s case manager and the relevant line manager/s. This will ensure continual follow up by the case manager and the development of ongoing support strategies for the client that can be built into their long-term safety plan. Strategies to increase protective factors should be introduced (e.g. regular visits with children organised etc.), as well as strategies to reduce risk factors (e.g. pain management plan developed for someone suffering with chronic illness).

6.0 DOCUMENTATION

DOCUMENTATION TO BE COMPLETED

6.1 FILE NOTES

Must be completed electronically and to a high standard. Workers are to ensure they put enough detail in the file note/s to ensure that clear reasons as to why a particular level of risk was assessed and the interventions implemented can be identified.

6.2 SUICIDE RISK ASSESSMENT

The Suicide Risk Assessment Form is to be completed after a client has been identified as at risk of suicide.

6.3 INCIDENT REPORT

The Incident Report is to be completed after an incident has occurred (e.g. ambulance called, client harmed themselves etc.) following the Incident Management Procedure.

6.4 EMPLOYEE SELF CARE

For STEPS to meet the needs of its client group it is imperative that workers look after themselves first. STEPS understands that working with people at high risk of suicide can at times be both challenging and rewarding. Workers are encouraged to implement their own self-care strategies in addition to accessing support provided by the organisation as required.

Organisational support available includes:

- Debriefing
- Supervision
- Counselling through the Employee Assistance Program
- Ongoing professional development (e.g. training, access to resources etc.)

7.0 RELATED DOCUMENTS

Document Name	Document Name
Suicide Risk Assessment Form (i052401)	Incident Management Procedure (i090700)
WHS Incident Report (i090201)	Incident Report (i090701)

IMS_i052400_SuidaIldtn_v3_240916_7824

1.7.9 Transitioning To/From STEPS

1.0 INTRODUCTION/GENERAL

We recognise the importance of each participant experiencing a planned and coordinated transition to and from STEPS Group of Companies (hereon referred to as STEPS). STEPS, in conjunction with the participants consent, will develop a transitional plan with the participant, and participants relevant supports, both current and exiting.

A Transition Plan (i052601) will be completed prior to exiting or entering a STEPS service or for temporary transitions, such as the participant requires hospitalisation or goes on holidays. This will be available to participants in the mode, format, and communication style best understood by the participant. STEPS will ensure all relevant parties (e.g. the participant, chosen supports, other providers) – where consent is given by the participant, are included in the development and implementation of the transition plan.

Where possible, STEPS will assist in the transition of the participant to ensure ongoing, seamless support is provided. Processes for transition to and from the provider are developed, applied, reviewed, and communicated within STEPS, to participants and relevant third parties.

1.0 DEFINITIONS

Word	Definition
Chosen Supports	The support network of a participant: for example, family, friends, carers, advocates, and other people who have a supportive relationship with a participant.
Participant	A person who meets the NDIS access requirements.
Transition	In this policy context, transition means transfer into a support from another provider, or transition out of a support to another provider, or temporary transition (i.e. hospitalisation or holidays), or transition out of a support to independence from that support (i.e. where a support is no longer needed), or transition into a support from independence from that support (i.e. where the participant's situation has changed and a new support to address that change is introduced).

2.0 TRANSITIONS FROM OTHER PROVIDERS TO STEPS

When a participant decides that they would like to leave another provider, and commence with STEPS, the following process applies:

2.1 Participant contacts STEPS to advise they would like to transition to STEPS Group.

2.2 We provide participant and their supporters information about STEPS and the supports we provide.

2.3 The participant and their supports are offered the opportunity to visit STEPS to view our service organisation, ask questions, see our facilities, and to have a preliminary discussion about goals and supports required.

2.4 Where an agreement is reached between the participant and STEPS, the participant is required to give notice to their current provider. If required and with the participants consent, STEPS can support and assist the participant to communicate their decision to the relevant parties.

2.5 Once notice has been given, we seek consent from the participant, to develop, in conjunction with the exiting provider, a Transition Plan (i052601). Once consent is received, a request to assist in the Transition Plan (i052601) and copies of any other relevant documentation is sent to the exiting provider.

2.6 STEPS will review any information provided and complete the relevant onboarding documentation as per the Service Entry Procedure (3111500), including the Service Agreement (3110016) STEPS will work with the exiting provider to agree on a timeline to complete the transition, to ensure the participant will not have any interruption to supports during this time.

2.7 Signed copies of the Service Agreement (3110016), transition and supporting documentation will be uploaded to the participant's file.

3.0 TRANSITIONS FROM STEPS TO ANOTHER PROVIDER

When a participant advises STEPS Group Australia that they would like to transition out to another provider, the following process applies:

3.1 The worker/manager commences the transition planning process by arranging a meeting time with the participant and their chosen supports.

3.2 The transition process is explained to the participant and their chosen supports.

3.3 The Transition Plan (i052601) and Participant Risk Assessment (3110089) is developed in conjunction with the participant or their chosen representative.

3.4 Consultation with support workers, assessors, support planners, and managers will occur in the developing and coordinating of transitional documentation. Where beneficial for the participant's transition, and with their consent, prior support plans and prior assessments may be provided. The participant's consent will be sought prior to contact with the other providers regarding transition planning and risk assessment.

3.5 A written agreement to transition out of STEPS is discussed, developed, and signed by STEPS, and the participant/guardian. Written consent will be requested to supply any additional information to the incoming provider.

3.6 The Transition Plan (i052601) and Participant Risk Assessment (3110089) are provided to the participant in the mode of communication and format best understood by them. With consent from the participant, a copy will also be provided to the incoming service.

4.0 TRANSITION TO INDEPENDENCE FROM STEPS

If the participant decides they would like to exit their current support to test independence or the participant no longer requires STEPS Group Australia's services, the following process applies:

4.1 Participant informs us that they would like to transition to independence or that a support is no longer required.

4.2 A Transition Plan (i052601) is developed with the participant, including discussing and listing any possible risks involved in the transition.

4.3 The participant and STEPS identify community-based mitigation strategies and supports to maximise opportunities for independence.

4.4 Where required, and with the participant's consent, STEPS arranges informal supports and other community-based interventions to maximise success, or we will support the participant to do this, themselves. These are documented in the Transition Plan (i052601).

4.5 The participant undertakes the activity unsupported, while the support worker observes, or the participant undertakes the activity unobserved and reports back to the support worker about successes and lessons.

4.6 The Transition Plan (i052601) is amended considering further risks, strategies, and opportunities identified through observation or self-report. The participant is provided with a copy of their Transition Plan (i052601) for future reference.

4.7 The participant exits STEPS with this being documented, and the participants file is closed. The participants personal information is retained for the minimum retention period in line with contractual and legislative requirements and managed in accordance with STEPS Privacy Policy (i010106).

5.0 RELATED DOCUMENTS

STEPS Social Business – Pathways College	
Document Name	**Document Name**
Individual Risk Assessment (5000014)	Participant Consent Form (5000021)
Service Agreement (5000030)	Service Entry (5000200)
Transition Plan (i052601)	
STEPS Community Support	
Document Name	**Document Name**
Consent to Manage your Personal Information (31100394)	Participant Risk Assessment (3110089)
Service Agreement (3110016)	Service Entry (3111500)
Transition Plan (i052601)	
Work Mates	
Document Name	**Document Name**
Service Agreement (3110016)	Service Entry (3111500)
Transition Plan (i052601)	

6.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	29 February 2024
Effective Date	7 March 2024	**Document Number**	i052600_v4_240307

(Uncontrolled when printed)

1.8 Managing Risk

Risk Management Framework (i052700)

1.8.1 Risk Management

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has developed an Integrated Management System (IMS) that describes the principles of risk management for the whole of the organisation, taking into account those risks recognised by STEPS and stated in the business plans, policies, and manuals. This procedure is based on those documents and is specific to risks that impact on corporate governance, work health and safety (WHS), and the environment. The STEPS risk management framework outlines the organisational approach to effectively manage risk and provides the foundation for STEPS risk culture.

The effective management of workplace risk is achieved through the identification of all organisational hazards including those hazards associated with work practices and aspects of work that impact on the environment. The assessment of the associated risks and the determination and implementation of appropriate controls will ensure elimination or mitigation of the risks. All risk assessments will be reviewed regularly for their appropriateness and currency; amended where required and re-issued in accordance with this procedure.

1.1 DEFINITIONS

Hazard	A thing or process that has a potential to cause illness, injury or death, or damage to plant, equipment, or the organisation.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation against benchmarks or standards
Risk	The possibility that harm (death, injury or illness) might occur when exposed to a hazard.
Risk Priorities	Establishing priorities for dealing with risk scores in accordance to their severity
Risk Control	The elimination or minimisation of the risk associated with the identified hazard using a recognised hierarchy of controls.

Likelihood	In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively, or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
Consequence	Outcome of an event affecting objectives: • An event can lead to a range of consequences. • A consequence can be certain or uncertain and can have positive or negative effects on objectives. • Consequences can be expressed qualitatively or quantitatively. • Initial consequences can escalate through knock-on effects.
Residual risk	Risk remaining after risk treatment that can contain unidentified risk and also be known as 'retained risk.'
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

Source: AS/NZS ISO 31000:2018 Risk management - Principles and guidelines; WHS Regulations 2011

1.2 ESTABLISHING THE CONTEXT

STEPS has evaluated and considered both the external and internal context of its core business, with focus on those factors that can significantly influence the design of the agreed risk management framework.

Evaluation of STEPS external context includes, but is not limited to:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive environment.
- key drivers and trends having impact on the business objectives; and
- relationships with, and perceptions and values of, external stakeholders

Evaluation of STEPS internal context includes, but is not limited to:

- governance, organisational structure, roles, and accountabilities.
- policies, objectives, and the strategies that are in place to achieve them.
- capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies).
- information systems, information flows and decision-making processes (both formal and informal).
- relationships with, and perceptions and values of, internal stakeholders.
- the organisation's culture.

- standards, guidelines, and models adopted by STEPS; and
- the form and extent of contractual relationships.

1.3 THE RISK MANAGEMENT PROCESS

The risk management process can be described as a series of steps:

- Risk Identification – the process of finding, recognising, and describing risk.
- Risk Analysis – determines the level of risk, expressed in terms of the combination of likelihood and consequences.
- Risk Evaluation – determining whether the risk is acceptable or tolerable, this also assists in the decision about risk treatment.
- Risk Treatment or control – is the process used to modify the risk and can involve taking or increasing risk to pursue an opportunity, or to deal with negative consequences through 'risk mitigation.'
- Monitoring and review – monitor the control measures to ensure they are working correctly to control the risks and that no other risks have been introduced.

2.0 CONDUCT A RISK ASSESSMENT

The following model sets out the steps of the risk management process, taking into account the regulatory framework that STEPS operates within.

2.1 FIGURE 1: MODEL OF RISK MANAGEMENT ADOPTED BY STEPS

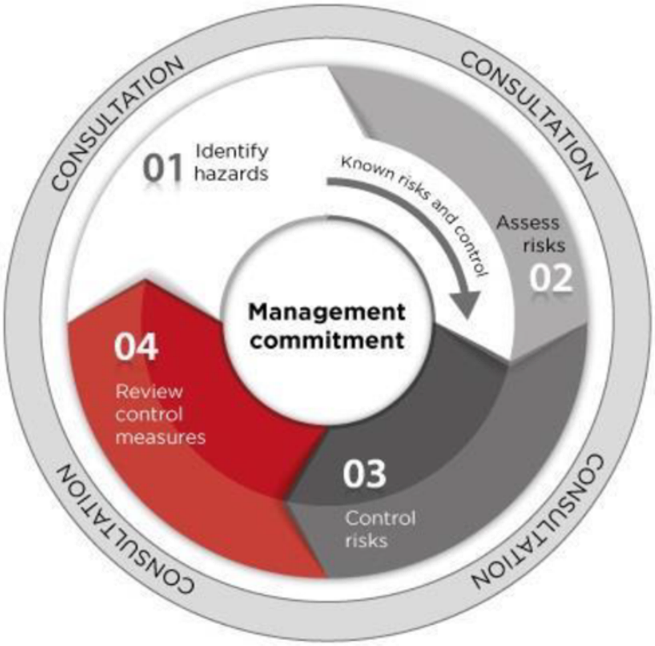


Figure 1 The risk management process

Source: How to Manage Work Health and Safety Risks Code of Practice 2011

2.2 HAZARD IDENTIFICATION

The identification of hazards must be a comprehensive and systematic process and must include all aspects of the workplace and work practice. Identification can occur through analysis of records (e.g., financial records, client complaints and feedback, worker complaints), workplace inspections, audits, incident reporting, OSI system, Rectification Action Plans and Risk Assessments.

Information and advice about hazards and risks relevant to particular industries and types of work is available from regulators, industry associations and technical specialists. Manufacturers and suppliers can also provide information about hazards and safety precautions for specific substances (Safety Data Sheets), plant or processes (instruction manuals).

2.3 CORPORATE RISK REGISTERS

A Corporate Risk Register (i050102) will list the corporate, WHS or environmental hazards relevant to the organisation, and will include risks, current controls, legislative controls, risk rating and future actions for each hazard.

2.4 CONSULTING WORKERS

A crucial part of hazard identification is the consultation with workers and Health and Safety Representatives (HSRs) about any corporate, WHS or environmental problems they have encountered in performing their work and any near misses or incidents that have not yet been reported.

2.5 HAZARD REPORTING

Hazards may be reported by workers at any time using the following means:

- Significant hazards where there is an immediate threat must be notified to relevant supervisor immediately verbally by phone or in person and recorded on the Hazard Report Form (i050103).
- All other hazards may be reported verbally to the relevant supervisor and recorded on the Hazard Report Form (i050103).

2.6 WHEN TO CONDUCT A RISK ASSESSMENT

A risk assessment may be undertaken by the subject matter specialist/s in consultation with other relevant parties on the following occasions if deemed necessary:

- Review of financial planning, audit reports.
- Prior to purchase of new plant or substances.
- Prior to changes to work procedures or environment.
- On introduction of new plant, substances or work processes or work environment.
- On changes to plant, substances or work processes or work environment.
- After any WHS incident resulting in injury, illness, or non-conformance.
- After audits and inspections are completed of plant, substances, work activities or work environment.
- Where amendments have occurred to legislation including Acts, Regulations, Codes of Practice, industry guidelines, Australian and relevant International Standards.
- Upon review of emergency provisions.

- Jobs or tasks that workers have identified as risky or hazardous.
- New jobs or tasks that present unknown or unspecified hazards.
- Where a product is imported from overseas and compliance to Australian Standards is required.

2.7 ASSESSING THE RISK

To determine if a hazard exists, relevant workers, the HSR and supervisor will complete the relevant Risk Assessment template.

Available templates and risk management processes on the Integrated Management System include:

- General Risk Assessment (i050105) – generic template
- Manual Task Checklist (i050401) - assessment of manual task activity with the tools, environment considered
- Hazardous Substances and Dangerous Goods Risk Assessment (i050502) - assessment of SDS and the activity undertaken
- Pre-purchase Risk Assessment for Plant (i080102) - review suppliers/manufacturers specifications prior to purchase.
- Job Safety Environmental Analysis (JSEA) Template (i050104) or Safe Work Procedures are to be developed for work activities that have been risk assessed.
- The Organisational System Improvement (OSI) System – for an OSI to be raised the risk rating must be low.

Where practical, a risk assessment should be planned and prepared some time before the job is undertaken, as controls and specialised equipment may be required and organised beforehand.

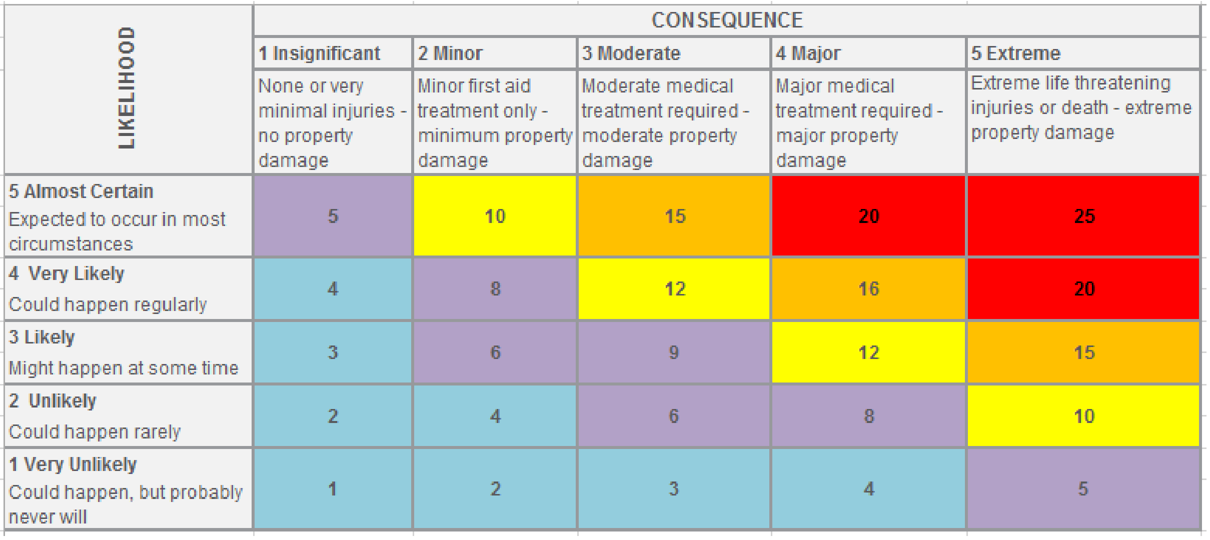
Those workers involved in conducting the Risk Assessment must be familiar with the principles of Risk Management and assess all risks in accordance with the established criteria of Australian Standards and relevant codes of practice as contained in this and related procedures.

Note that a number of high-risk activities are described in the WHS Regulations 2011 that include manual tasks, noisy environments, work at heights. The controls specified in the Regulations must be followed at all times and used as preventative actions in risk assessments.

2.8 HOW TO CONDUCT A RISK ASSESSMENT

A Risk Assessment can be conducted using the General Risk Assessment (i050105) template and following the instructions listed on this form. Once the hazards have been identified and the risks have been assessed, controls must be chosen in accordance with the table of risk priorities and hierarchy of controls listed next. Scores are obtained by selecting the likelihood rating and recording in column ‘L’ on the record sheet of the risk assessment template. Next select the consequence.

Note that the consequence must take account of the worst-case scenario; hence if research of records of illness and injury suggest death is a consequence of a certain activity when uncontrolled then the high rating must be chosen, i.e., extreme.

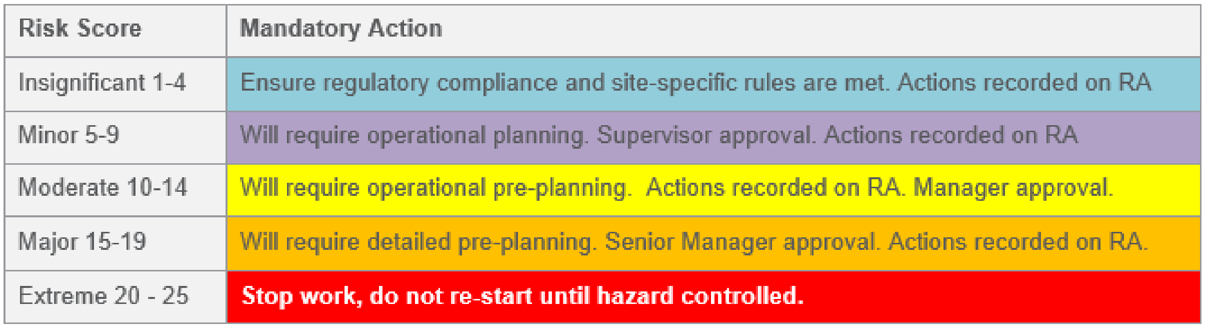


LIKELIHOOD	CONSEQUENCE				
	1 Insignificant None or very minimal injuries - no property damage	2 Minor Minor first aid treatment only - minimum property damage	3 Moderate Moderate medical treatment required - moderate property damage	4 Major Major medical treatment required - major property damage	5 Extreme Extreme life threatening injuries or death - extreme property damage
5 Almost Certain Expected to occur in most circumstances	5	10	15	20	25
4 Very Likely Could happen regularly	4	8	12	16	20
3 Likely Might happen at some time	3	6	9	12	15
2 Unlikely Could happen rarely	2	4	6	8	10
1 Very Unlikely Could happen, but probably never will	1	2	3	4	5

2.9 CONTROLLING THE RISK

The table of risk priorities below gives assistance in deciding if the final risk rating after addition of controls has reduced the risk level low enough to commence work, or whether there is a need to investigate further controls to lower the rating.

2.10 TABLE OF RISK PRIORITIES



Risk Score	Mandatory Action
Insignificant 1-4	Ensure regulatory compliance and site-specific rules are met. Actions recorded on RA
Minor 5-9	Will require operational planning. Supervisor approval. Actions recorded on RA
Moderate 10-14	Will require operational pre-planning. Actions recorded on RA. Manager approval.
Major 15-19	Will require detailed pre-planning. Senior Manager approval. Actions recorded on RA.
Extreme 20 - 25	**Stop work, do not re-start until hazard controlled.**

Risk Assessment Matrix and Rationale sourced from ISO13000:2018 Risk Management Principles & Guidelines

2.11 CHOOSING CONTROLS BASED ON THE HIERARCHY OF CONTROLS AND IN ACCORDANCE WITH RISK PRIORITIES

Once the risks have been assessed, controls must be chosen in accordance with the hierarchy below. Always attempt to eliminate the hazard and if not practical, identify and implement substitution; engineering or separation should be looked at next.

Note that administrative controls and personal protective equipment should be implemented in conjunction with a higher order control where possible. In all instances, elimination is the preferred option and should be considered wherever possible.

2.12 HIERARCHY OF CONTROLS TABLE WITH EXAMPLES OF RISK TREATMENTS

Control	Description	Examples
Eliminate	The removal of hazards from the workplace completely	• Removing an obstruction out of a doorway or hallway. • Safely dispose of unwanted chemicals.
Substitute	Replacing a hazardous substance or work practice with a less hazardous one.	• Replacing a telephone handset with a headset. • Substituting a hazardous chemical with a less dangerous one.
Isolate	Isolating the hazard from the rest of the workplace.	• Enclosing or guarding dangerous equipment. • Installing screen or barriers around hazardous areas.
Engineering	The redesign of equipment or work processes to minimise the hazard.	• The installation of RCD (Residual Current Devices) safety switches in the workplace. • Use trolleys to move heavy loads.
Administration	Introduce administrative controls to minimise the hazard	• Procedure changes • Installation of signs and warning labels.
PPE	The use of appropriate Personal Protective Equipment (PPE)	Gloves, respirators, ear plugs, hard hats, sun hats and other protective equipment.

Once the controls have been chosen, the residual risk can be calculated. If the risk score cannot be immediately reduced to score 1-12, the assessment must be signed off by the supervisor and WHS Officer before work begins.

2.13 ADDING THE RISK ASSESSMENT TO THE RISK REGISTER

Once the risk assessment is completed the manager is responsible for emailing the risk assessment to the WHS Officer. The WHS Officer will:

- File in the correct location in ‘O’ Drive using the appropriate categorisation, and,
- add the completed risk assessment to the Risk Register to enable reminders to be sent out for reviews and to record who has been trained in the risk assessment.

2.14 ONGOING EVALUATION AND MONITORING

Once a risk control option has been implemented, the relevant supervisor must review effectiveness of the risk control measures implemented and record any required changes. A full risk analysis must again be undertaken if a risk control measure is determined as being ineffective as per this procedure.

Hazards may change over time. The supervisor or nominated person will update risk assessments according to section 2.7. All Risk Assessments and associated documents will be reviewed regularly as notified by the WHSO from the dates recorded in the risk register.

When the review is completed, the manager is responsible for emailing the reviewed risk assessment to the WHS Officer who will add to the risk register as per 2.13 above.

2.15 TRAINING AND EDUCATION

The Risk Management process forms part of the Corporate WHS Induction. All workers who are required to undertake risk assessments will receive training on how to conduct a risk assessment, including identification of hazards, assessment of risks, applying suitable controls in accordance with the established hierarchy of controls; and establishing a regime for monitoring and reviewing the effectiveness of the controls.

Supervisors are responsible for ensuring all new workers receive training in Risk Assessments or JSEAs prior to commencing tasks and will record this information on a Training Attendance record. A copy must be saved in the ‘Training’ folder under the site name in the WHS folder in ‘O’ drive.

The Training Attendance records must be emailed to the WHS Officer who will record the staff names against the risk assessment to enable reporting and reminders to retrain following an update to the incident register.

Workers may receive training in new Risk Assessments and JSEAs at Team Meetings.

3.0 RECORD KEEPING

Approved Risk Assessments and JSEAs will be available on the under the WHS folder in ‘O’ drive. This folder will contain all current risk assessments filed by entity, service stream and risk category.

The WHS Office will send out monthly reports on what risk assessments require review and when staff training needs to occur.

All superseded risk assessments will be saved in an archive folder in the Risk Assessment folder in ‘O’ drive.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Corporate Risk Register (i050102)	General Risk Assessment (i050105)
Hazard Report Form (i050103)	Job Safety Environmental Analysis (JSEA) Template (i050104)
Hazardous Substance and Dangerous Goods Risk Assessment (i050502)	Manual Task Checklist (i050401)
Pre-Purchase Risk Assessment for Plant (i080102)	

5.0 GOVERNANCE

Document Owner	Executive Manager - Human Resources	**Approval Date**	5 July 2022
Effective Date	20 July 2022	**Document Number**	i050100_v7_220720

(Uncontrolled when printed)

1.9 Information Security Management

STEPS understands and acknowledges that information is an extremely valuable asset as it may contain:

- Personal and sensitive information of customers, participants, and students, or
- Commercial information about services, brands and processes.

You can help in achieving a successful Information Security Management System by complying with the policies and procedures contained in this section of the STEPS Quality Manual (SQM).

By applying a risk management process and implementing the controls STEPS will preserve the confidentiality, integrity, and availability of information which will enable interested parties and stakeholders to have confidence in the way STEPS manages information security risks.

To access a print friendly version of the Information Security Management System (ISMS) Manual (6000004) click ***here***.

Link to Security Do's and Don'ts Cheat Sheet (6000006)

ICT Help Desk

Phone: (07) 5458 3052

Mobile: 0418 736 990

Please email your queries through to helpdesk@stepsgroup.com.au or contact us via 07 5458 3096.

STEPS Support Networks

Support Area	Contact
ConnX	Contact HR (07) 5458 3096

ESS Security & Logins	Helpdesk
ESS	1300 305 520
iCase	(03) 8533 7700
Networks & Computers	Helpdesk
SEE Online	Contact Education & Training (07) 5436 6000
WiseNet	Contact Education & Training (07) 5436 6000
Suns Systems Support	1300 658 608 sun_systems@pa.com.au

1.9.1 Policies

Enter topic text here.

1.9.1.1 Acceptable Use Policy

INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS”.

This policy sets out the rights and responsibilities of all users who have access to STEPS’ Information and Communication Technology (ICT) services, including but not limited to all digital and electronic information storage and communication processes including telephone, computer networks, computer desktop equipment, laptops, mobile devices, electronic mail systems, internet, and intranet web services. Users include, but are not limited to, STEPS employees, contractors, visitors, voluntary and temporary staff.

POLICY STATEMENT

GENERAL

a) All users of STEPS’ ICT services must comply with:

- STEPS’ information security policies.
- applicable laws, including (but not limited to) copyright, intellectual property, breach of confidence, defamation, privacy, contempt of court, harassment and cyberstalking, vilification and anti-discrimination legislation, and workplace surveillance legislation.
- show restraint in the consumption of STEPS’ ICT services.
- observe professional integrity; and

b) Users are responsible for:

- all activities that originate from STEPS' ICT services.
- all information sent from, solicited, or viewed from STEPS' ICT services.
- publicly accessible information placed on a computer using their account; and
- taking precautions to deter the introduction of malicious software with STEPS' ICT services.

c) Users shall:

- only use a STEPS' ICT service for the purpose for which it was allocated.
- keep access codes, passwords, other authentication and identity data associated with STEPS' ICT services confidential in accordance with the requirements of the Password Procedure (6001100).
- prevent the use of allocated STEPS' ICT services by others; and
- ensure STEPS' ICT services are physically protected from security threats and environmental hazards.

d) Permission to use and access STEPS' ICT services is personal and non-transferable.

e) Users must not:

- use STEPS' ICT services data for personal financial gain or profit.
- use STEPS' ICT services to access gambling, pornography, weapons, cryptocurrency, personal VPN, filter avoidance, hacking, hate speech, illegal activities, illegal drugs, illegal downloads, terrorism.
- use STEPS' ICT outside Australia, unless prior approval has been obtained from the Managing Director
- reveal or publish STEPS' restricted, or confidential information, personal information which could identify a specific individual (including but not limited to mailing or email address, phone numbers, login IDs, social media accounts, digital images, or IP addresses).
- be in breach of copyright laws, license agreements and contracts.
- publish material or enter into contractual agreements except in accordance with STEPS' policies and procedures.
- violate or attempt to violate any law or regulation; and
- engage in conduct which damages a person or a company's reputation.

f) STEPS is committed to a workplace free from harassment and discrimination.

STEPS will not tolerate employees using the internet, email, or any form of social media to publish, send or forward any material which breaches harassment, or discrimination policies, or relevant legislation.

Intention is irrelevant. If the use of ICT services offends, humiliates, or intimidates another person it may breach this policy and/or the relevant legislation.

STEPS or an individual user may be held liable for improper or unlawful use of ICT services.

A user must not use STEPS' ICT services to:

- discuss or comment on the physical appearance of other employees, customers, or users, whether they are a recipient of the message or not.
- make comments of a sexual, sexist, or racist nature or make inferences or comments about a person's sexual preferences.

- make degrading comments, whether based on race, disability, gender, political beliefs, religion, pregnancy, marital status, age, or family status, etc; and
- use abusive or offensive language.

This list is incomplete but provides examples of inappropriate types of conduct.

g) Users must not use STEPS' ICT services to store, display or transmit objectionable material in a way which is:

- offensive, indecent, obscene, menacing, violent or abusive.
- intended to incite criminal activities or instruct others in how to commit criminal activities.
- sexually explicit, pornographic, obscene, or suggestive or could otherwise be considered objectionable.

h) STEPS do not permit or condone the publication of defamatory material. If a user of STEPS ICT services publishes, transmits, or passes on any statement, comment, or innuendo about another individual or organisation which cannot be justified at law they may be liable to an action for defamation and will be required to indemnify STEPS against all actions, proceedings, claims and costs resulting from these actions / damages.

i) **Users must not breach intellectual property laws:**

- most graphics, text, computer software and other material available on the internet are protected by intellectual property laws. Much of STEPS' internal material is similarly protected.
- users must take care not to breach intellectual property law by copying, distributing, or otherwise using protected material. It is an offence under Commonwealth law to copy software or other materials from the internet without authority. It is immaterial whether you are copying for personal convenience or for monetary gain. All users should read and comply with any copyright notices when accessing individual sites and prior to printing. Further care should be taken not to infringe copyright by transmitting copyright material to other parties.
- if protected material is copied; both the user and STEPS could be exposed to serious penalties. In some countries, infringement of a person's intellectual property rights can attract criminal penalties.

j) In addition to the terms of existing confidentiality obligations and agreements, employees, visitors, volunteers, and contractors with access to and use of STEPS' ICT services must:

- not disclose confidential information relating to STEPS' business or affairs unless authorised to do so in writing.
- not disclose personal information about STEPS' employees other than in the course of their employment.
- access only those systems and data for which they have been authorised.
- secure files and reports used or created.
- be responsible for protecting the secrecy of their personal authentication information. This includes ICT user account name, computer log-in and password, staff identification number and any other information which uniquely identifies an authorised user to grant them access to ICT services.
- in the case of remote login services, ensure that their login details are always kept confidential.

k) If you find yourself connected to a site that contains sexually explicit, offensive, or inappropriate material, you must disconnect from that site immediately. In addition, unacceptable material may not be viewed, downloaded, archived, stored, distributed, edited, or recorded using STEPS' ICT services or company resources.

l) A user must not examine, disclose, copy, rename, delete, or modify software or data without the express or implied permission of its owner.

m) A user must not monopolise STEPS' ICT services. Specifically, prohibited example of monopolisation would be overloading STEPS' ICT services with excessive quantities of information.

n) A user must not waste consumable resources, damage resources, or behave in a manner that inconveniences other users of STEPS' ICT services.

o) A user must not attempt to circumvent system security, network security or any protection or resource restrictions placed on an account.

p) A user must not attempt to capture or decode passwords or access codes, read, or capture any data without authority.

q) A user must not attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software, or data.

r) A user must not install software which has not been authorised in writing by STEPS. This includes and is not limited to file sharing, online collaboration, gaming, crypto-mining, gambling, personal VPN, website hosting, file manipulation, proxy anonymisation, video streaming, torrenting, and social media.

s) A user must not attach any unauthorised device or signal to STEPS' ICT services.

t) A user must not connect any equipment providing off-site access to STEPS' ICT services without the prior authorisation of the delegated STEPS employee.

u) A user must not tamper with or move installed STEPS' ICT services without the authorisation of the delegated STEPS employee.

v) When using mobile devices (e.g. laptops, tablets, mobile phones) users must take all reasonable steps to ensure that STEPS' business information is not compromised (refer to Mobile Device Policy (6002100).

w) When using a wireless broadband connection device, it is the responsibility of STEPS staff with wireless internet or remote access privileges to the STEPS corporate network to ensure they adhere to corporate policies.

x) Users must report all incidents affecting security to STEPS' ICT department as quickly as possible.

y) All ICT equipment and software identified for disposal or sale, must be checked to ensure all resident data is copied and deleted prior to disposal or sale.

NETWORK MONITORING

All STEPS users must be aware of the following:

a) Network monitoring is an inherent part of the effective operation of the network. It is required for security and performance, for the purpose of detecting unauthorised use of the network and for the purpose of detecting crime and other infringements of legislation (e.g., copyright infringement).

b) All data, information and electronic files kept on STEPS' ICT infrastructure are not regarded as private.

c) The network may be monitored to record and / or analyse data relating to the transmission of information on the network for the purpose of investigating problems, legislative infringements, or misuse of corporate information.

d) The ICT Department has the right to perform regular monitoring, scanning, and probing to detect problems or misuse and to take remedial action as a result. The criteria for taking remedial action will be based on any one or more of the following:

- the result of regular monitoring of the volume of network traffic and other factors that may have an impact on network performance and reliability.
- as requested by the STEPS Executive Leadership Team.
- as instructed by the Police or an order of a court of Australia.
- receiving a complaint from an individual or organisation.
- the result of scanning for viruses.
- the result of scanning for software that may pose a security risk to the network and / or other network users.
- the result of vulnerability probes/testing.

e) Action(s) taken because of monitoring, scanning and probing could be any one or more of the following:

- reporting misuse to the relevant line manager/supervisor which may result in a formal warning or dismissal.
- disabling the network connection associated with the equipment.
- disabling the user's account and making the user's home directory files inaccessible to the STEPS user.
- notifying the user of a problem and requesting certain actions to be taken within a stated period.
- further analysis of the source of network traffic to determine the nature of the suspected problem (e.g. high volume of network traffic being caused by file sharing programs).
- deleting, removing and cleaning of files on the file server.

f) If a user believes that the ICT department's representative is behaving unreasonably in the application of its monitoring, they may report this to the relevant line manager/supervisor.

ELECTRONIC MAIL RULES

a) Email messages should be kept as short and specific as practicable.

b) Subject to any standard specified by STEPS, material that must not be transmitted by email includes:

- restricted data; inappropriate personal observation about STEPS, its employees or other persons including contractors, volunteers, visitors and customers, participants, and students.
- advertising material (other than advertisements by STEPS or of specific relevance to STEPS' business).
- material of a private nature including political or religious material.
- any material which could reasonably be considered to commercially disadvantage STEPS or that is commercial in confidence.
- solicitation of donations or subscriptions to political causes.
- content used to promote discrimination based on race, colour, national origin, age, marital status, sex, political affiliation, religion, disability, or sexual preference.
- offensive text or pictures (e.g. pornography, racism, sexism, obscenities, insults, sarcasm); content that may reasonably be considered offensive, threatening, or intimidating; defamatory statements, rumours, and gossip, about individuals or organisations.

- responses to irritating email or junk mail just to retaliate. Responding to junk email confirms your email address for future junk email and may enable the downloading of malicious software.

c) Email is provided primarily for STEPS business use and may be used in legal proceedings.

d) Email must not be used to:

- send any form of chain letter.
- send mail so that it appears to have come from someone else.
- automatically forward mail to an internet site or personal email account.
- send unsolicited email to others without proper business purpose.
- It is specifically prohibited to use email to harass, send abusive messages, defame or to transmit pornography.

e) Responsible personal use is permitted, provided it is reasonable and is not detrimental to STEPS' image.

f) The laws of copyright, privacy and freedom of information apply to email communications and all users are responsible for compliance with those laws.

Refer to the Email Procedure (6000400) for more information.

SOCIAL MEDIA USAGE RULES

Please refer to STEPS' Social Media Procedure (e210200).

ABANDONMENT

All STEPS users must be aware of the following:

a) Access to STEPS' ICT services will be disabled after 45 days of inactivity.

b) STEPS' ICT services will be deleted should STEPS be unable to satisfactorily confirm an ongoing need for the assigned STEPS' ICT services.

PERSONAL USE

The computers, electronic media and services provided by STEPS are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

PARTICIPATION IN ONLINE FORUMS

Employees should remember that any messages or information sent on STEPS-provided facilities to one or more individuals via an electronic network - for example, Internet mailing lists, bulletin boards, and online services - are statements identifiable and attributable to STEPS.

STEPS recognises that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a disability problem by consulting members of a news group devoted to the specific disability area.

DECLARATION

I understand that I have no expectation of privacy when I use any of the STEPS' ICT services. I am aware that violations of this Policy on appropriate use of the email and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability.

I further understand that my use of the email and Internet may reflect on the image of STEPS to our consumers, competitors, and suppliers and that I have responsibility to maintain a positive representation of STEPS. Furthermore, I understand that this agreement can be amended at any time.

I, ____ (full name) have read, understood and agree to comply with the policies, rules and conditions outlined in this Acceptable Use Policy.

NAME			
SIGNATURE		DATE	

This policy was ratified by the Board on 28 May 2024.

(Uncontrolled when printed).

To access a print friendly version of this Policy please click here.

1.9.1.2 Access Control Policy

INTRODUCTION

STEPS Group of Companies is hereinafter referred to as "STEPS".

POLICY STATEMENT

ACCESS TO STEPS' ICT SERVICES, FACILITIES, AND INFRASTRUCTURE

Current employees of STEPS are automatically afforded authorised user status. In addition, any person falling under the following categories may apply and receive authorisation from the Technology & Cyber Security Manager to use STEPS' ICT services, facilities and infrastructure and become recognised as an authorised User:

- A contractor undertaking work for STEPS under the provisions of a legal contract.
- A member of a collaborative venture in which STEPS is a partner.
- A visiting professional who is undertaking activities approved by STEPS' Executive Leadership Team (ELT).
- A member of STEPS' Board.

EXTERNAL ACCESS

Connections to STEPS' ICT Services, Facilities and Infrastructure from external sources may only be performed via methods approved by the Technology & Cyber Security Manager.

The following methods of connection are currently approved:

- For publicly provided services access will be provided using industry standard means. Examples include: The https protocol for web services.
- Any connection requiring authentication against ICT Services, Facilities or Infrastructure must be performed using encrypted means, and may only be performed by an authorised user.

Examples include:

- STEPS authorised remote desktop services.
- STEPS ICT authorised and configured corporate VPN solution.
- HTTPS encryption on any web site.

External parties who require access to ICT Infrastructure to maintain systems must be granted time-limited access that does not exceed the time required to provide the support / maintenance activity and must only use approved access methods.

ACCOUNT CREATION

Account creation occurs when a person becomes an authorised user. This process indicates a person has a current relationship with STEPS.

Account creation will only occur when a person has been registered:

- as a current staff member, volunteer, or contractor, through STEPS approved on-boarding processes; or
- At the direction of the ELT.

Account creation will not occur before a person is recognised as an authorised User.

Accounts will not become active until the commencement of employment or engagement as a contractor has occurred.

CHANGE OF EMPLOYMENT

The Human Resources (HR) Team are required to notify the ICT Team of any change in position, entity, role, or responsibilities of any employee. The HR Team will submit an approved ticket through the ICT Service and Support Portal to notify the ICT Team of the appropriate employee details.

ACCOUNT DEACTIVATION

Account deactivation shall occur upon termination of an authorised user’s relationship with STEPS. This may occur via, but is not limited to, the following events:

Staff:

- Termination of employment; and
- Resignation.

Contractor / Visiting Professional:

- Conclusion of contract or consultant services; and
- Conclusion of collaborative project.

The Executive Manager – Human Resources is responsible for ensuring that the offboarding workflow occurs and that the ICT team is notified of the required account deactivation immediately.

ACCOUNT PRIVILEGES

Assignment of account privileges is based on the principal of least privilege. An authorised user will be provided with access sufficient for their role and will not be afforded greater levels of access.

If an authorised user's role changes, their access rights may also change to reflect the requirements of their new role.

ACCOUNT AUDITING

Bi-annual auditing of user accounts will be performed by STEPS to identify and revoke non-active, unused, or non-authorised accounts; or to perform the reallocation or revocation of privileges. This review of access rights for users will be conducted across all systems including those maintained by third parties and not administered by ICT. ICT are responsible for ensuring that these reviews are conducted twice a year, ideally in March and August. The Information Asset Owner will assist in the review process as required, with ICT completing the process within the JIRA platform.

ACCOUNT SECURITY

Account details must be made secure as per the requirements of the Password Procedure (6001100), which forms part of STEPS' ICT security framework.

NETWORK ACCESS AND AUTHENTICATION

Access to the STEPS networks is managed in accordance with the Network Access and Authentication Procedure (6000800).

ADMINISTRATOR ACCESS REQUIREMENTS

Administration of ICT services, facilities and infrastructure may only be carried out by:

- ICT personnel authorised by the Technology & Cyber Security Manager; or
- A person who holds responsibility, via their current position description, for the maintenance and management of data, or an ICT Service.

Administrators must be a current employee of STEPS or an approved third-party support role. Administration rights, access and group membership held by an individual shall be immediately revoked upon cessation or suspension of employment with STEPS, change in role, or termination of contractual support arrangements with STEPS.

SEPARATION OF DUTIES

Administrators of ICT services, facilities and infrastructure shall not hold rights greater than those required of their role.

Separation of duties and responsibilities will be used to ensure no one person can circumvent normal auditing processes.

The minimum implementation will be to separate the roles of Systems Administrator from database administration for all systems holding confidential or financial information, or any system identified as a corporate system.

GENERIC ACCOUNTS

The use of shared, guest, anonymous and other such generic user accounts shall be avoided where possible. If guest or anonymous accounts must be used to access STEPS' ICT services and facilities, they must be supported by a process that identifies the user of the account, such as a record of account allocation.

Wherever possible, generic accounts must have the minimum rights and privileges required to perform their role and must not be used gain write access to any corporate systems or stores of confidential information.

Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. A User does not directly initiate the task, nor is a user the direct recipient of the information. This includes automatic downloads and other linkages for data transfer.

This policy was ratified by the Board on 6 June 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here

1.9.1.3 Backup Policy

INTRODUCTION

STEPS Group of Companies is hereinafter referred to as "STEPS".

This policy sets out the data backup requirements to ensure integrity and availability of important data is maintained.

POLICY STATEMENT

DATA BACKUPS

STEPS will perform data backups for important data and systems. In supporting this statement, STEPS will:

a) Identify with the business on what data, software, and systems are included in a backup process.

b) Set out a backup frequency and retainment process to support business continuity.

c) Ensure backups are made resilient and secure.

d) Storage of data backups are retained in a remote location from any STEPS office.

BACKUP ACCESS

STEPS will prohibit the unauthorised access to backups. Unprivileged and privileged accounts will not be able to access their own backup data and the backup data of other accounts or STEPS users. Designated backup administrators are exempt from this requirement.

STEPS will have at least one immutable data repository for important data to ensure deletion cannot occur. All backup data will be encrypted.

TESTING AND RESTORATION

STEPS will perform regular validation and testing of data restoration from various backup data repositories.

DATA BACKUP DESTRUCTION

STEPS will perform regular review of data backups to ensure appropriate destruction activities occur validation and testing of data restoration from various backup data repositories.

This policy was ratified by the Board on 6 June 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here

1.9.1.4 Clean Desk and Clear Screen Policy

INTRODUCTION

STEPS Group of Companies is hereinafter referred to as “STEPS”.

This policy sets out how all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use, or a STEPS user leaves his/her workstation. STEPS users include, but are not limited to, STEPS employees, contractors, visitors, voluntary and temporary staff.

POLICY STATEMENT

CLEAR DESK

a) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

b) Any confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

c) File cabinets containing confidential information must be kept closed and locked when not in use or when not attended.

d) Keys used for access to confidential information must not be left at an unattended desk.

e) Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

f) Printouts containing confidential information should be immediately removed from the printer.

g) Upon disposal confidential documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.

h) Whiteboards containing confidential information should be erased.

i) Ensure portable computing devices such as laptops and tablets are secured within a locked office or building.

j) Treat mass storage devices such as CD, DVD or USB drives as confidential and secure them in a locked drawer.

CLEAR SCREEN POLICY

a) If the authorised person is not at their workstation, all confidential information must be removed from the screen to not be visible or accessible by unauthorised persons.

b) Computer workstations and laptops must be locked when workspace is unoccupied (use windows key + L or F4).

c) Computer workstations and laptops must be shut completely down at the end of the workday.

d) In the case of short absence (up to 15 minutes), the clear screen policy is implemented by locking the screen with a password. If the person is absent for a longer period (over 2 hours), the clear screen policy is implemented by logging out of all systems and turning off the workstation.

This policy was ratified by the Board on 6 June 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here

1.9.1.5 Cryptographic Control Policy

INTRODUCTION

STEPS Group of Companies is hereinafter referred to as “STEPS”.

This policy sets out requirements for the use of cryptography to protect the confidentiality, integrity, and authenticity of STEPS data, systems, and users.

POLICY STATEMENT

In accordance with the Data Classification Procedure (6000300), as well as legal and contractual obligations, STEPS must protect individual systems or information by means of the following cryptographic controls:

a) Controls applied in accordance with the Australian Signals Directorate (ASD) approved cryptographic algorithms.

b) STEPS asset owners to which cryptographic controls are applied are responsible for appropriate application of individual cryptographic controls.

KEY MANAGEMENT

Key management is critical to the success of an implementation of encryption technology. The following guidelines apply to the company's encryption keys and key management:

Management of keys must ensure that data is available for decryption when needed:

a) Cryptographic keys must have secured copies.

b) Cryptographic keys must never be transmitted in clear text, considered confidential, and never shared to unauthorised parties.

c) Physical key generation materials must be destroyed within five business days.

d) Cryptographic keys must be used and changed in accordance with the Password Procedure (6001100).

e) When user encryption is employed, minimum key length is 10 characters.

The Technology & Cyber Security Manager is responsible for prescribing the following rules regarding key management:

a) Generating private and public cryptographic keys.

b) Activation and distribution of cryptographic keys.

c) Defining the time limit for the use of keys and their regular updating (in accordance with risk assessment).

d) Archiving inactive cryptographic keys which are necessary for encrypted electronic archives.

e) Destruction of cryptographic keys.

DATA TRANSMISSION AND STORAGE

Full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition must be implemented. When made available or insufficient security exists for the protection of data communicated in the clear over network infrastructure, encryption should be used.

This policy was ratified by the Board on 6 June 2023.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here

1.9.1.6 Information Security Policy

STEPS Group of Companies hereinafter referred to as “STEPS”. is committed to establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

STEPS understands and acknowledges that information is an extremely valuable asset as it may contain personal and sensitive information of our customers, participants, and students, as well as commercial information about services and processes. We acknowledge that as an organisation, we can minimise information security risks through the preservation of confidentiality, integrity, and availability of information. This gives confidence to interested parties that risks due to potential incidents are adequately managed.

In order to achieve this, the following information security objectives have been established:

- Information security risks are understood and treated to be acceptable to STEPS
- The confidentiality of personal and business information is protected
- The integrity of company records is preserved; and
- Public web services and internal networks remain available to meet the organisation's needs.

To achieve these objectives, we shall act to:

- Communicate this policy to all existing employees and to new employees upon commencement
- Comply with all legislative and other requirements which are relevant to STEPS
- Make our commitment to information security and confidentiality visible to all interested parties; and
- Maintain an Information Security Management System which meets the requirements of ISO 27001.

This policy, together with the objectives and targets set, will be reviewed on an annual basis to ensure that it remains relevant suitable to the operations of STEPS.

This policy was ratified by the Board on 28 May 2024.

To access a print friendly version of this Policy please click here.

1.9.1.7 Mobile Device Policy

INTRODUCTION

STEPS Group of Companies is hereinafter referred to as “STEPS”.

This policy is intended to protect the security and integrity of STEPS’ data and technology infrastructure.

POLICY STATEMENT

Mobile computing equipment includes all kinds of portable computers, smartphones, memory cards, USB devices and other mobile equipment used for storage, processing and transferring of data, which may be taken off-premises only after obtaining authorisation in accordance with the Acceptable Use Policy (6001700).

Special care is to be taken when mobile computing equipment is placed in vehicles, public spaces, hotel rooms, meeting places, conference centres, and other unprotected areas outside the organisation’s premises.

Personnel taking mobile computing equipment off-premises will abide by the following:

a) If possible, where unattended, should be physically locked away, or special locks (e.g., Kensington Lock) should be used to secure the equipment.

b) When using mobile computing equipment in public places, the user must take care that data cannot be read by unauthorised persons.

c) Updates of patches and other system settings are performed by STEPS.

d) Protection against malicious code is installed and updated by STEPS.

e) The person using mobile computing equipment off-premises is responsible for saving to the STEPS corporate network at the first opportunity. They also need to ensure that all reasonable steps are taken to preserve data if they are working on files that are saved on their local computer, if using other cloud-based tools the back-ups will automatically be completed.

f) Connecting to communication networks and data exchange must reflect the sensitivity of data and is performed by using a VPN through a mobile hotspot and not public Wi-Fi networks. Refer to the VPN Procedure (6001500) for more information.

g) Information on portable computers must have whole disk encryption enabled in accordance with the Data Classification Procedure (6000300).

h) In case mobile computing equipment is left unattended, the equipment must be physically secured, protected from damage, and any technical access controls employed.

i) The Technology & Cyber Security Manager is responsible for organising training and raising awareness of persons who are using mobile computing equipment outside the organisation’s premises.

MOBILE DEVICE SECURITY

j) The use of encryption either for the entire device or for data identified as sensitive is required on all mobile devices.

k) The usage of unapproved application stores is prohibited.

l) Use of anti-malware software (where supported) on mobile devices is required.

m) Devices connecting to corporate networks or storing and accessing company information shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier.

n) To prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the company network.

o) The company’s strong password policy is passwords must be at least 14 characters.

p) Device must lock itself with a password or PIN if it is idle for 15 minutes.

q) Circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) is prohibited. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

r) Mobiles and tablets belonging to employees that are for personal use only are not allowed to connect to the network.

s) Employees’ access to company data is limited based on user profiles defined by ICT and automatically enforced.

t) Employee’s device may be remotely wiped if:

   a. The device is lost or stolen.

   b. Termination of employment.

   c. ICT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

BRING YOUR OWN DEVICE (BYOD)

BYOD is for mobile phones only. STEPS employees must agree to the terms and conditions set forth in this policy. At a minimum, the mobile phone must have a 4-digit lock code or biometric lock to connect to STEPS' email system.

a) Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

b) Employee is expected to always use their own devices in an ethical manner and adhere to the company's Acceptable Use Policy (6001700) as outlined above.

c) Employee is personally liable for all costs associated with his or her device.

d) Employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

e) STEPS' reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

WORKING FROM HOME & REMOTE

Teleworking relates to information and communication equipment used to enable employees to perform their work outside the organisation. This does not include the use of mobile phones outside the organisation's premises.

Working from home must be authorised by HR in accordance with the Flexible Working Arrangements Procedure (e250100), the line manager/supervisor is responsible for communicating the rules to ensure the following:

a) Protection of mobile computing equipment as specified in the previous section.

b) Prevention of unauthorised access by persons living or working on the location where the work-related activity is performed.

c) Appropriate configuration of the local network used for connecting to the Internet (i.e. Wi-Fi password).

d) Protection of the organisation's intellectual property rights, either for software or other materials that may be protected by intellectual property rights.

e) Process for return of data and equipment in the case of termination of employment.

f) Minimum level of configuration of the facility where work-related activities will be performed.

g) Permitted and forbidden types of activities.

This policy was ratified by the Board on 28 May 2024.

(Uncontrolled when printed)

To access a print friendly version of this Policy please click here.

1.9.2 Procedures

Enter topic text here.

1.9.2.1 Awareness, Training & Competency Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 PURPOSE

The aim of this procedure is to identify the training and competency needs based on various internal and external requirements, determining course content, selecting training providers, assessing training effectiveness and conducting system inductions/awareness training. The procedure ensures that all staff are made aware of all ISMS procedures, position responsibilities and other company or job requirements.

1.2 DEFINITIONS

Competency, Training & Awareness	The standards require that organisations determine the necessary competence for workers and then organise the appropriate ISMS training.
Asset Owner	Person or entity with accountability for an asset and authority to make decisions about the security controls to protect the confidentiality, integrity, and availability of an asset.

1.3 RESPONSIBILITIES

Position	Responsibilities
Executive Manager – Human Resources	a) Determine the level of experience, competence, and qualification necessary for personnel to carry out activities required by the ISMS. b) Determine training needs. c) Plan for personnel to receive adequate training as required. d) Ensure training organisations are accredited by the business prior to delivery of training. e) Ensure training records are maintained in the personnel files.
Asset Owner	a) Ensure current staff and contractors have the appropriate qualifications and competency to perform work. b) Ensure new staff and contractors are inducted into STEPS. c) Assess the effectiveness of any training that personnel have undergone.

All Staff	a) Comply with instructions to attend training and apply the information to work activities.

2.0 PROCEDURES

2.1 DETERMINING COMPETENCY REQUIREMENTS

The Executive Manager - Human Resources shall identify competency requirements for STEPS personnel. This shall be based on the requirements of legislation, project requirements and the risks associated with plant and equipment in use. New personnel will be evaluated against their corresponding minimum criteria when applying for the position, upon beginning in the role, and during probation.

Competency requirements shall be determined for each position (including management) and recorded in their position descriptions.

Review of competency requirements shall occur whenever the following occur:

a) Changes occur to legislation.

b) New plant, work processes or systems are introduced.

c) New projects are planned.

2.2 DETERMINING COURSE CONTENT

The relevant manager organising the training will determine the course content based on:

a) Client requirements.

b) Information and recommendations from industry associations.

c) Information from action requests, strategic initiatives, and consultation with staff.

d) Information provided on legislative changes.

e) Privileged access to systems and/or financial information.

2.3 SELECTION OF TRAINING PROVIDERS

Training providers will be accredited and selected in the same way as other suppliers of services in accordance with the Outsourcing Procedure (6001000).

2.4 MAINTAINING TRAINING RECORDS

The Executive Manager - Human Resources is responsible to ensure that the Human Resources Information System (HRIS) is maintained and make certain that information on all staff training is available centrally and notification of any recurrent training is in effect. In addition, all training records (certificates of attainment, attendance etc.) must be kept in the personnel file.

2.5 ASSESSMENT OF TRAINING EFFECTIVENESS

The relevant manager will consult with staff, individually or as a group, to discuss the effectiveness of the training they have undergone. The information will be noted in the personnel files as well as in the training provider’s file.

2.6 INDUCTION & AWARENESS

All employees will be inducted when they start working with STEPS. The induction will be recorded in their personnel files and an Induction Checklist - Employee (i070101) is completed to ensure no aspect is missed inadvertently. This induction will include going through the ISMS awareness training, which is conducted annually.

All contractors will also be inducted before they commence work on-site. This forms part of the supplier accreditation and will be part of the supplier's terms of engagement. The hiring manager will ensure all new staff and contractors are inducted before commencing work.

3.0 RELATED DOCUMENTS

Document Name	Document Name
Induction Checklist - Employee (i070101)	Outsourcing Procedure (6001000)

4.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6000100_v2_230601

(Uncontrolled when printed)

1.9.2.2 Communication Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as "STEPS."

1.1 PURPOSE

This communication procedure has been developed to ensure effective engagement and communication with respect to the ISMS within STEPS.

1.2 DEFINITIONS

Interested party	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

1.3 RESPONSIBILITIES

Position	Responsibilities
Executive Leadership Team	• Providing adequate resources for the implementation of this procedure
Chief Administrative Officer	• Ensure that communication methods are implemented in accordance with this procedure

	• Ensure that the Policies and Procedures Sub-Committee review these communication methods on an annual basis to ensure that additional external and internal communication methods are incorporated.

2.0 PROCESS

This procedure is aimed at interested parties, both internal and external, contract and permanent, who have a part to play in the operation and development of the ISMS within STEPS. A full description of the interested parties of the ISMS is set out in the *Information Security Risk Register*.

The interested parties include:

- Board of Directors
- Suppliers
- Customers, participants, and students
- Regulatory bodies
- Customer user groups
- Employees of the organisation
- Contractors providing services to the organisation.
- Emergency services
- General public
- Media
- Neighbours
- Building Manager.

3.0 COMMUNICATION TOPICS

The communication procedure is intended to outline the key items of information that is communicated in the following main areas:

- The business environment in which the ISMS operates, including significant changes as and when they occur
- The overall framework of the ISMS including the vision, policies, plans and objectives that are to be achieved
- How the information security measures in place relate to the needs of the business, both now and going forward
- How the ISMS is intended to capture and fulfil the business requirements for information security
- The statutory, regulatory, and contractual requirements and constraints within which the ISMS must operate
- Updates on how plans are progressing towards meeting the defined objectives of the ISMS
- Awareness of information security issues and risks and our approach to addressing them

The level of detail required in the above areas will vary across the interested parties involved.

4.0 COMMUNICATION METHODS

There are several established communication methods in place within STEPS and these will be used where possible. These include:

Interested Party	Subject of Communication	Method(s)	Frequency
Executive Leadership Team	Information security strategy High level risk management Policy setting High level reporting	Management Review Meeting Quality and Risk Sub-Committee Meetings Policies and Procedures Sub-Committee Meetings	Biannually Monthly Monthly
Chief Administrative Officer Technology & Cyber Security Manager	Information security awareness Security requirements for new ICT systems Review of risks and issues Reviews of security breaches	ISMS Working Group Meetings	Quarterly
Employees	Communication of Information Security Policy Ad-hoc reminders when important events occur e.g., breaches Warnings and awareness	Electronic notifications	As required
Suppliers and partners	Information security policy Contractual requirements Supplier obligations Suggestions for improvement	Emails to suppliers	Annually
Customers, participants, and students	Purpose of the ISMS Information security policy Controls in place	Described on website	Ongoing
Government agencies and regulators (including Department of Education, Skills and Employment, Department of Social Services)	Purpose of the ISMS Information security policy Controls in place	Described on website	Ongoing

5.0 FEEDBACK ABOUT COMMUNICATION

For each interested party, a designated relationship owner will be agreed who is responsible for obtaining feedback on the success of communication and managing the relationship on an ongoing basis. Relationship owners are shown in the following table:

Interested Party	Relationship Owner
Executive Leadership Team	Chief Administrative Officer
ISMS Working Group	Chief Administrative Officer
Employees	Executive Manager – Human Resources
Suppliers and partners	CFO
Customers, participants, and students	General Managers, Principals, Program Managers, Site Manager
Government agencies and regulators (including Department of Education, Skills and Employment, Department of Social Services)	ELT
Other interested parties	Chief Administrative Officer

Feedback about the success of communication will be collected, evaluated and, if appropriate, incorporated into the procedure as soon as possible.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Awareness, Training & Competency Procedure (6000100)	Management Review Meeting Minutes (6000001)
Information Security Risk Register *Located under* ISMS-Registers	Information Security Policy (6002300)

7.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023

Effective Date	1 June 2023	Document Number	6000700_v2_230601

(Uncontrolled when printed)

1.9.2.3 Confidential Data Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS”.

2.1 DEFINITIONS

Authentication	A security method used to verify the identity of a user and authorise access to a system or network.
Encryption	The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
Removable Data Device	A data storage device that utilises flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
Two-Factor Authentication	A means of authenticating a user that utilises two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

2.0 PROCEDURE

2.1 TREATMENT OF CONFIDENTIAL DATA

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Procedure (6000300).

2.2 STORAGE

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

2.3 TRANSMISSION

Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside STEPS' network. Confidential data must not be left on voicemail systems, either inside or outside STEPS' network, or otherwise recorded.

2.4 DESTRUCTION

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: destroyed after placement in secure document destruction bin.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the Technology & Cyber Security Manager must be notified.

2.5 USE OF CONFIDENTIAL DATA

A successful Confidential Data Procedure is dependent on the users knowing and adhering to STEPS' standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access by labelling data.
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her Line Manager / Supervisor.
- Users must report any suspected misuse or unauthorised disclosure of confidential information immediately to his or her Line Manager / Supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to STEPS' Outsourcing Procedure (6001000) for additional guidance.
- If confidential information is shared with a third party, STEPS must indicate to the third party how the data should be used, secured, and, destroyed. Refer to STEPS' Outsourcing Procedure (6001000) for additional guidance.

2.6 SECURITY CONTROLS FOR CONFIDENTIAL DATA

Confidential data requires additional security controls to ensure its integrity. STEPS requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for confidential data transmitted internal or external to STEPS. Confidential data must always be stored in encrypted form, whether such storage occurs on a user machine, server, laptop, or any other device that allows for data storage.
- Physical Security. Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.

- Printing. When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be in secured areas.

- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be in secured areas.

- Emailing. Confidential data must not be emailed inside or outside STEPS without the use of strong encryption.

- Mailing. If confidential information is sent outside STEPS, the user must use a service that requires a signature for receipt of that information. When sent inside STEPS, confidential data must be transported in sealed security envelopes marked "confidential."

- Discussion. When confidential information is discussed, it should be done in non-public places, and where the discussion cannot be overheard.

- Confidential data must be removed from documents unless its inclusion is necessary.

- Confidential data must never be stored on non-company-provided machines (i.e., home computers).

- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

2.7 EXAMPLES OF CONFIDENTIAL DATA

The following list is not intended to be exhaustive but should provide STEPS with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer tax file numbers or personal information

- Medical and healthcare information

- Customer data

- Product and/or service plans

- Network diagrams and security configurations

- Communications about corporate legal matters

- Board documents

- Passwords

- Bank account information and routing numbers

- Payroll information

- Credit card information

- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

2.7 APPLICABILITY OF OTHER POLICIES

This document is part of STEPS' cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology and Cyber Security Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Data Classification Procedure (6000300)	Outsourcing Procedure (6001000)

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6000200_v2_230601

(Uncontrolled when printed)

1.9.2.4 Data Classification Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS”.

1.1 DEFINITIONS

Authentication	A security method used to verify the identity of a user and authorise access to a system or network.
Backup	To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption	The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
Mobile Data Device	A data storage device that utilises flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
Two-Factor Authentication	A means of authenticating a user that utilises two methods: something the user has, and something the user knows. Examples are email/text/SMS security PIN, smart cards, tokens, or biometrics, in combination with a password.

2.0 PROCEDURE

2.1 DATA CLASSIFICATION

Data residing on corporate systems must be continually evaluated and classified into the following categories:

Public: includes already-released marketing material, commonly known information etc. There are no requirements for public information.

Internal: includes data for basic business operations which is available to all employees (non-confidential).

Restricted: any information to which some employees have access relevant to their role and/or responsibilities e.g., client information, management, financial, human resources. Restricted data is usually critical to effective operations and is often treated as confidential where personal information needs to be protected. It is extremely important to identify restricted data for security and backup purposes. Most data will fall into this category.

2.2 DATA STORAGE

The following guidelines apply to storage of the different types of company data.

2.2.1 Public

There are no requirements for public information.

2.2.2 Internal

Internal data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

2.2.3 Restricted

Restricted data must be stored on a server that gets the most frequent backups (refer to the Backup Policy (6002000) for additional information). System or disk-level redundancy is required.

2.2.4 Confidential

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

2.3 DATA TRANSMISSION

The following guidelines apply to transmission of the different types of company data.

2.3.1 Public

There are no requirements for public information.

2.3.2 Internal

No specific requirements apply to transmission of Internal Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

2.3.3 Restricted

There are no requirements on transmission of restricted data, unless the data in question is also considered confidential, in which case the applicable procedure statements would apply.

2.4 CONFIDENTIAL

Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside STEPS' network. Confidential data must not be left on voicemail systems, either inside or outside STEPS' network, or otherwise recorded.

2.5 DATA DESTRUCTION

The following guidelines apply to the destruction of the different types of company data.

2.5.1 Public

There are no requirements for public information.

2.5.2 Internal

There are no requirements for the destruction of Internal Data, though shredding is encouraged.

2.5.3 Restricted

There are no requirements for the destruction of Restricted Data, though shredding is encouraged. If the data in question is also considered confidential, the applicable procedure statements would apply.

2.5.4 Confidential

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: Use of document destruction bins required
- Storage media (CD's, DVD's): physical destruction is required
- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the Technical & Cyber Security Manager must be notified.

2.6 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technical & Cyber Security Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Backup Policy (6002000)	Confidential Data Procedure (6000200)

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6000300_v2_230601

(Uncontrolled when printed)

1.9.2.5 Email Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 DEFINITIONS

Auto Responder	An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.
Certificate	Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.
Data Leakage	Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems.
Email	Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.
Encryption	The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.
Mobile Device	A portable device that can be used for certain applications and data storage. Examples are laptops or Smartphones.

Password	A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
Spam	Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.
Smartphone	A mobile telephone that offers additional applications, such as PDA functions and email.
Two Factor Authentication	A means of authenticating a user that utilises two methods: something the user has, and something the user knows. Examples are email, text/SMS; smart cards, tokens, or biometrics, in combination with a password.

2.0 PROCEDURE

2.1 PROPER USE OF COMPANY EMAIL SYSTEMS

Users are asked to exercise common sense when sending or receiving email from company accounts. Additionally, the following applies to the proper use of STEPS email system.

2.2 SENDING EMAIL

When using a company email account, email must be addressed and sent carefully. Users should keep in mind that STEPS loses any control of email once it is sent external to STEPS network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help STEPS avoid the unintentional disclosure of sensitive or non-public information.

2.3 PERSONAL USE AND GENERAL GUIDELINES

Some personal usage of company email systems is permitted as long as

a) such usage does not negatively impact the corporate computer network, and

b) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to STEPS may not be sent via email, regardless of the recipient, without proper encryption.
- It is company practice not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that the topics above may be covered in more detail in other sections of this procedure.

2.4 BUSINESS COMMUNICATIONS AND EMAIL

STEPS uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognise that email sent from a company account reflects on STEPS, and, as such, email must be used with professionalism and courtesy.

2.5 EMAIL SIGNATURE

An automated email signature is added when email is sent from company mail clients. This email signature includes the user’s:

- Name
- Title
- Company name
- Phone number(s)
- Fax number if applicable
- URL for corporate website

Email signatures may not include personal messages (political, humorous, etc.).

2.6 AUTO-RESPONDERS

STEPS recommends the use of an autoresponder if the user will be unavailable for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

2.7 MASS EMAILING

STEPS makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with STEPS' employees or customer base) and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is STEPS' intention to comply with applicable laws governing the sending of mass emails. For this reason, it is recommended that approved tools such as Mailchimp or SurveyMonkey be used, however in order to be consistent with good business practices, STEPS requires that email sent to more than twenty (20) recipients external to STEPS have the following characteristics:

a) The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honoured immediately.

b) The email must contain a subject line relevant to the content.

c) The email must contain contact information of the sender.

d) The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

Note that emails sent to company employees, existing customers, or persons who have already inquired about STEPS' services are exempt from the above requirements.

2.8 OPENING ATTACHMENTS

Users must use care when opening email attachments. Viruses, Trojans and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected email attachments
- Never open email attachments from unknown sources
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted emails can hide a malicious URL.

STEPS may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

2.9 MONITORING AND PRIVACY

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to transmission and storage of files, data, and messages. STEPS reserves the right to monitor all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

2.10 COMPANY OWNERSHIP OF EMAIL

Users should be advised that STEPS owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by STEPS and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

2.11 CONTENTS OF RECEIVED EMAILS

Users must understand that STEPS has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, STEPS may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her Line Manager/Supervisor.

2.12 ACCESS TO EMAIL FROM MOBILE PHONES

Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. This can present several security issues, particularly relating to the storage of email, which may contain sensitive data, on the phone. Users are not to access, or attempt to access, STEPS' email system from a mobile phone without the permission of his or her Line Manager/Supervisor and IT.

Note that this section does not apply if STEPS provides the phone and mobile email access as part of its remote access plan. In this case, permission is implied. Refer to the Mobile Device Policy (6002100) for more information.

2.13 EMAIL REGULATIONS

Any specific regulations (industry, governmental, legal, etc.) relating to STEPS' use or retention of email communications must be adhered to.

2.14 EXTERNAL AND/OR PERSONAL EMAIL ACCOUNTS

STEPS recognises that users may have personal email accounts in addition to their company-provided account. The following sections apply to non-company provided email accounts:

2.14.1 Use For Company Business

Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-company-provided email account.

2.14.2 Access From Steps Network

Users are prohibited from accessing external or personal email accounts from the corporate network.

2.14.3 Use For Personal Reasons

Users are strongly encouraged to use a non-company-provided (personal) email account for any non-business communications.

2.15 CONFIDENTIAL DATA AND EMAIL

The following sections relate to confidential data and email:

2.15.1 Passwords

As with any company passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Procedure (6001100). STEPS may further secure email with certificates, two factor authentication, or another security mechanism.

2.15.2 Emailing Confidential Data

Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

STEPS requires the encryption of email that contains confidential information, this is particularly important when the email is sent to a recipient external to STEPS.

Further guidance on the treatment of confidential information exists in STEPS' Confidential Data Procedure (6000200). If information contained in the Confidential Data Procedure (6000200) conflicts with this procedure, the Confidential Data Procedure (6000200) will apply.

2.15.3 Company Administration Of Email

STEPS will use its best effort to administer STEPS' email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.

2.15.4 Filtering Of Email

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, STEPS will filter email at the Internet gateway and/or the mail server, to filter out spam, viruses, or other messages that may be deemed:

A. Contrary to this procedure, or

B. A potential risk to STEPS' ICT security.

No method of email filtering is 100 percent effective, so the user is asked additionally to be cognizant of this procedure and use common sense when opening emails.

2.15.5 Additionally, many emails and/or anti-malware programs will identify and quarantine emails that it deems suspicious. email disclaimers

The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in STEPS' risk reduction efforts. STEPS requires the use of email disclaimers on every outgoing email, which must contain the following notices:

- The email is for the intended recipient only
- The email may contain private information
- If the email is received in error, the sender should be notified, and any copies of the email destroyed.

An example of such a disclaimer is:

NOTE: *This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorised review, use, disclosure, or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying to this email, and destroy all copies of the original message.*

2.15.6 Email Deletion

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this procedure is to keep the size of the user's email account manageable and reduce the burden on STEPS to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email to hide a violation of this or another company procedure. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

2.15.7 Retention and Backup

Email should be retained and backed up in accordance with the applicable procedures, which may include but are not limited to the: Data Classification Procedure (6000300), Confidential Data Procedure (6000200), Back Up Policy (6002000), and Records Management Procedure (i020300).

Unless otherwise indicated, for the purposes of backup and retention, email should be considered internal use data as per the Data Classification Procedure (6000300).

2.15.8 Address Format

Email addresses must be constructed in a standard format in order to maintain consistency across STEPS. The companies recommended format is:

- FirstnameFirstInitialLastname@stepsgroup.com.au

The intent of this procedure is to simplify email communication as well as provide a professional appearance.

2.15.9 Email Aliases

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for company email, as well as (often) the names of company employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

- sales@companydomain.com
- techsupport@companydomain.com
- pr@companydomain.com
- info@companydomain.com.

STEPS may or may not use email aliases, as deemed appropriate by the Technical & Cyber Security Manager and/or executive team. Aliases may be used inconsistently, meaning: STEPS may decide that aliases are appropriate in some situations but not others depending on the perceived level of risk.

2.15.10 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive company email. Accounts will be set up at the time a new hire starts with STEPS, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

2.15.11 Account Termination

When a user leaves STEPS, or his or her email access is officially terminated for another reason, STEPS will disable the user's access to the account by password change, disabling the account, or another method. STEPS is under no obligation to block the account from receiving email and may continue to forward inbound email sent to that account to another user or set up an auto-response to notify the sender that the user is no longer employed by STEPS.

2.15.12 Storage Limits

As part of the email service, email storage may be provided on company servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the Technical & Cyber Security Manager. Storage limits may vary by employee or position within STEPS.

2.15.13 Prohibited Actions

The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:

- Send any information that is illegal under applicable laws.
- Access another user's email account without:
  a) the knowledge or permission of that user - which should only occur in extreme circumstances.

  b) the approval of company executives in the case of an investigation.

  c) when such access constitutes a function of the employee's normal job responsibilities.
- Send any emails that may cause embarrassment, damage to reputation, or other harm to STEPS.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.

- Knowingly misrepresent STEPS' capabilities, business practices, warranties, pricing, or policies.
- Conduct non-company-related business.

STEPS may take steps to report and prosecute violations of this procedure, in accordance with company standards and applicable laws.

2.15.14 Data Leakage

Data can leave the network in several ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to STEPS' control of its data.

Unauthorised emailing of company data, confidential or otherwise, to external email accounts for the purpose of saving this data external to company systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her Line Manager / Supervisor rather than emailing the data to a personal account or otherwise removing it from company systems.

STEPS may employ data loss prevention techniques to protect against leakage of confidential data.

2.15.15 Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. STEPS asks that the user limit email attachments to 10Mb or less.

The user is further asked to recognise the additive effect of large email attachments when sent to multiple recipients and use restraint when sending large files to more than one person.

2.16 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable

3.0 ENFORCEMENT

This procedure will be enforced by the ICT Manager and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities are suspected, STEPS may report such activities to the appropriate authorities. If any provision of this procedure is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Back Up Policy (6002000)	Confidential Data Procedure (6000200)

Data Classification Procedure (6000300)	Mobile Device Policy (6002100)
Password Procedure (6001100)	Records Management Archiving Procedure (i020300)

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6000400_v2_230601

(Uncontrolled when printed)

1.9.2.6 Guest Access Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS”.

1.1 DEFINITIONS

Account	A combination of username and password that allows access to computer or network resources.
Guest	A visitor to STEPS premises who is not an employee.

2. PROCEDURE

2.1 GUEST LAPTOPS

The ICT Department is responsible for maintaining a pool of guest laptops that have been provisioned with the standard operating environment. The ICT Department maintain an inventory of these laptop and are responsible for tracking the details of who the laptops are issued to and the tracking the return of laptops.

2.2 GRANTING PROVISION OF GUEST LAPTOP

Guest laptops will be provided on a case-by-case basis by the Technical & Cyber Security Manager to any approved person who can demonstrate a reasonable business need to access the STEPS corporate network. Requests should be lodged through ICT Helpdesk to ensure that they are recorded and actioned by ICT.

Note: There is a Guest Wi-Fi Network that is provided to facilitate access to the internet for guests, but that network is separate from the STEPS corporate network.

2.3 AUP ACCEPTANCE

Guests must agree to and sign STEPS' Acceptable Use Policy (6001700) (AUP) before the Guest Laptop is provided.

2.4 SECURITY OF GUEST MACHINES

Guests and the relevant STEPS manager will be responsible for ensuring that the Guest Laptop is kept at a STEPS location and not taken offsite.

2.5 MONITORING OF GUEST ACCESS

Since guests are not employees of STEPS, they are not considered trusted users. As such, STEPS will monitor guest access to ensure that STEPS' interests are protected, and the Acceptable Use Policy (6001700) is being adhered to.

2.6 GUEST WI-FI TERMS OF SERVICE

Guests should also be referred to the Guest Wi-Fi Terms of Service (6000501) if required.

3. ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4. RELATED DOCUMENTS

Document Name	Document Name
Acceptable Use Policy (6001700)	Guest Wi-Fi Terms of Service (6000501)
Network Access and Authentication Procedure (6000800)	

5. GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	11 April 2024
Effective Date	23 April 2024	**Document Number**	6000500_v3_240423

(Uncontrolled when printed)

1.9.2.7 ICT Change Management Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 PURPOSE

The purpose of this document is to set out the STEPS process of change management in relation to information processing facilities and systems that affect information security.

The objective is to ensure that changes to ICT services and their associated components are recorded and then evaluated, authorised, prioritised, planned, tested, implemented, documented, and reviewed in a controlled manner.

A change request may arise for many reasons, including the following:

- An incident or problem
- New hardware installation
- New functionality
- ICT Infrastructure upgrades
- New or changed legislation
- Changed business requirements or direction
- Retirement of service

A change request must be assessed for impact (including information security implications) and resource requirements before being considered by the Change Committee (CC). To assist with impact assessment, the identification of related systems/components affected by the proposed change and also input from other affected support groups may be required.

After assessment, if the change is deemed acceptable it will be provided to the Executive Leadership Team (ELT) for authorisation. Once implemented the change will be reviewed and subject to the findings of the review, closed.

2.0 CATEGORIES OF CHANGE

The following categories of change will be used:

- Normal
- Emergency
- Major

Each of these categories will require different processing as follows:

2.1 NORMAL CHANGES

These are “business as usual” changes which are expected to make up the majority of the change requests that are logged and handled through the change management process as described in this document. Although not emergencies, they will be prioritised in order that resources can be allocated in as effective a manner as possible.

2.2 EMERGENCY CHANGES

Whilst all changes likely to be required should be foreseen and planned, there will be occasions when business requirements demand that changes be made in an emergency situation. Such changes are those requests which impact on internal or external 'live' systems and require implementation in order to resolve (or prevent) a current high priority incident or problem. In such cases a change request must be raised immediately even if the full change details are not available, and the Quality and Risk Sub-Committee must be notified. This is to ensure that all parties are aware at the earliest opportunity.

From initial logging of the change, the principles of the normal change management process should be observed as far as is realistic, however, as an emergency changes may require swift approval from the ELT an Emergency Quality and Risk Sub-Committee meeting may be held.

If an emergency change cannot be formally authorised after reasonable efforts have been made to follow the process (e.g., out of hours) a decision by a member of the ELT may be made as to whether this change will be implemented. However, details of the change must still be recorded, and the change management process followed retrospectively to ensure that records are maintained accurately, and the success or failure of the change can be reviewed.

Where timescales allow it, the CC in collaboration with the relevant support groups will ensure the following:

- Sufficient staff and resources are available to action and support the change request
- Back-out or exit plans have been documented and passed to the change Implementer
- As much testing as possible of the emergency change has been completed

When an emergency change request is logged the Executive Manager – Companies Support Services will do the following:

- Assess who should attend the emergency Quality and Risk Sub-Committee. Communicate with each member of the Quality and Risk Sub-Committee whatever means is appropriate (face-to-face, telephone, email) to obtain a combined impact assessment

The remainder of the process will then continue but under the auspices of the Quality and Risk Sub-Committee rather than the Change Committee i.e., as quickly as possible whilst retaining control and managing risk

Changes processed as emergencies will be reviewed by the ELT on a regular basis to ensure that they are genuine emergencies and do not arise from a lack of forward planning.

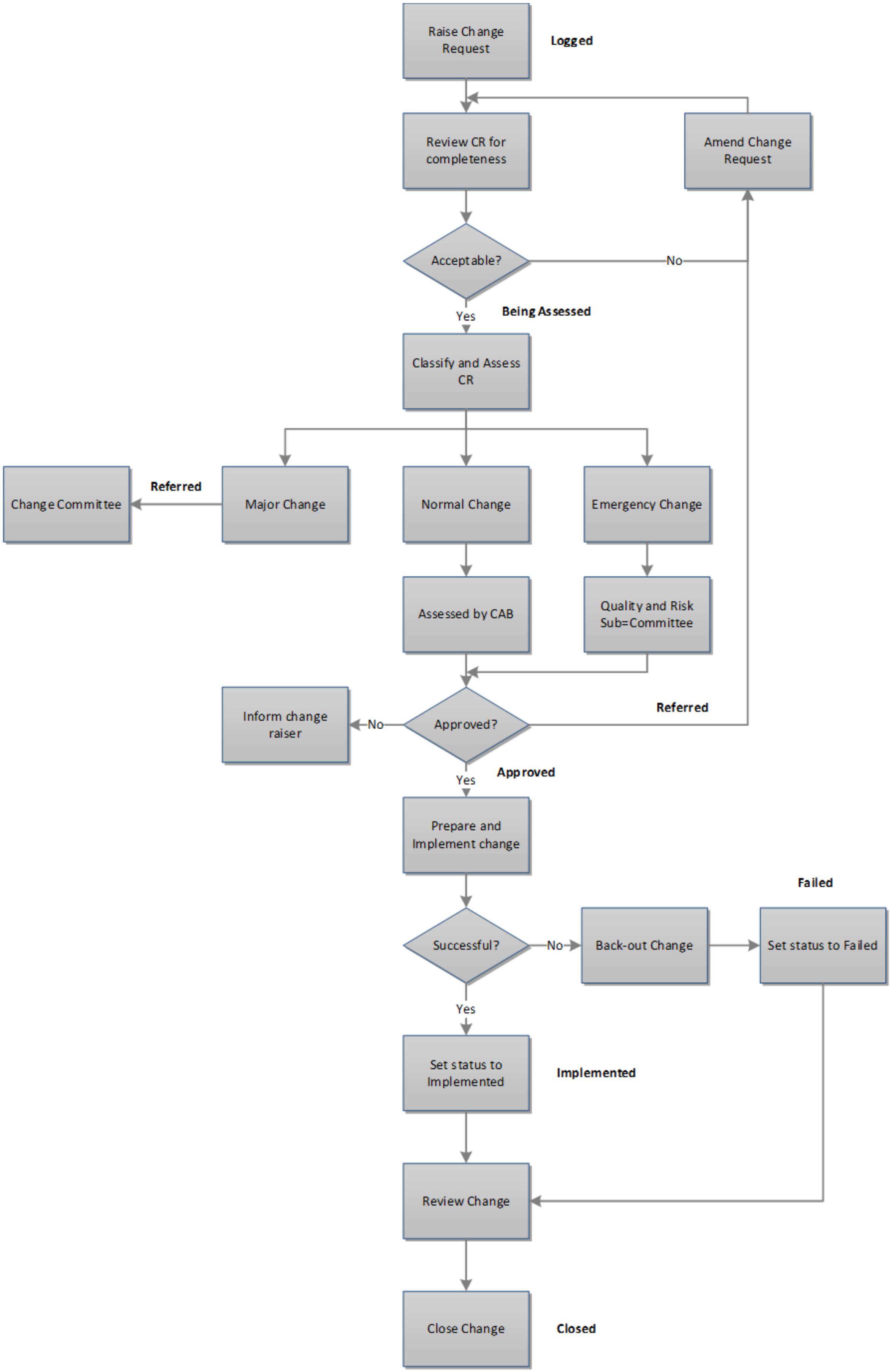
2.3 MAJOR CHANGES

Major changes will be logged within the change management process but referred to the Change Committee as their scope and implications will generally encompass a wider audience. They will then be raised as projects with their own business case, project team and budget.

However, note that a project may generate further change requests that may be managed within the change management process as normal changes.

3.0 CHANGE MANAGEMENT PROCESS

3.1 PROCESS DIAGRAM


Raise Change Request
Logged
Review CR for completeness
Amend Change Request
Acceptable?
No
Yes
Being Assessed
Classify and Assess CR
Change Committee
Referred
Major Change
Normal Change
Emergency Change
Assessed by CAB
Quality and Risk Sub=Committee
Inform change raiser
No
Approved?
Referred
Yes
Approved
Prepare and Implement change
Failed
Successful?
No
Back-out Change
Set status to Failed
Yes
Set status to Implemented
Implemented
Review Change
Close Change
Closed

3.2 PROCESS NARRATIVE FOR MAJOR AND EMERGENCY CHANGE

Step	Role	Description
Raise change request	Change Initiator	Create a change record within the service desk systems (e.g., OSI, Help Desk) detailing all the required information
Classify and Review CR for completeness	Project Manager	The change request needs to be checked that all the required information has been entered. The change should be referred or rejected if it is: 1. Totally impractical 2. A duplicate change requests 3. Incomplete
Amend CR	Change Initiator	The addition of further information if required or clarification of existing information
Classify and Assess CR	Project Manager	Assess whether the change request is Major or an Emergency
Refer to Quality and Risk Sub-Committee	Project Manager/ Project Management Office	If the change is categorised as Major, then it will be referred to the Change Committee as a possible project
Assess a Normal change request for technical and business risk	Service Desk Systems	The implications of the proposed change are assessed from a business and a technical point of view. This should include the timing and impact on information security, capacity, service continuity plans and release management, amongst other areas
Assess an Emergency change request for technical and business risk	Quality and Risk Sub-Committee	The change is assessed as for a Normal change but in an accelerated timescale either face to face or via telephone, email etc.
Approve, reject or refer the change request	Change Committee / ELT	Change Committee will refer back to change initiator if more information required ELT will Approve if OK, reject if not.
Schedule Change	Change Committee	Inform the Change Initiator of the result of the approval process and enter the change on the change schedule
Prepare and Test Change	Change Committee / ICT Team	Plan the mechanics of the change and ICT Team will test it where appropriate e.g., in a test environment

Implement Change	Change Implementer	Make the change on the date and time scheduled. Test to ensure it has worked successfully
Back-Out Change	Change Implementer	Remove the change if unsuccessful
Report Success	Change Implementer	Inform the Project Manager that the change was implemented successfully
Review Change	Change Committee	Review the change records to ensure that no related incidents or problems have arisen since the change was made
Close Change as successful	Change Committee	Close the change record with a status of successful
Close Change as Unsuccessful	Change Committee	Close the change record with a status of unsuccessful

3.3 PROCESS ROLES AND RESPONSIBILITIES

Change Initiator

- May be within the business (business generated changes) or within ICT (Infrastructure changes)
- Responsible for identifying the need for a change and providing the required information to allow the change request to be assessed
- Works with the change builder to define the exact requirements of the change
- May be involved in user acceptance testing of the change once built

Change Committee

- Consider major change requests
- Work as a team, and invite input from other internal stakeholders to understand the change request and its requirements
- Use project management framework to develop Business Case and define scope and resources
- Consult with ICT Team to understand impact and risks to information assets that may be affected by the change
- Provide information to ELT for approval
- Communicate with change initiator
- Identify Project Manager and support the implementation of the change once authorised
- Support the governance of change within STEPS

Project Manager

- Owner of the ICT change management process
- Responsible for identifying improvements to the process and ensuring it is adequately resourced

- Provides information regarding the success rates of the process
- Performs the initial check and classification of changes

Quality and Risk Sub-Committee

- Reviews and approves or rejects emergency changes based on the information provided
- Ensuring that all changes to the production environment are adequately assessed for risk avoidance and impact, including on information security

Executive Leadership Team (ELT)

- Approving changes presented that meet business needs and conform to change management rules for major changes
- Confirming the priority of authorised changes
- Verifying where possible that resources are committed to executing authorised changes to agreed schedules
- Resolving conflicts in the change schedule
- Taking corrective action against any person/group who attempts to circumvent the change management process
- Reviewing historical records of changes to ensure that the process is running as required

ICT Change Implementer

- Works with the change initiator to define the requirements in more detail
- Creates the items necessary for the change (e.g., new, or revised software programs)
- Performs system testing and liaises with the change originator to perform UAT
- Plans the details of the change, tests it prior and post implementation
- Verifying that valid test plans are produced for changes in order to protect the production environment
- Provides feedback to the Project Manager on the status of the change

3.4 CHANGE COMMITTEE (CC) MEETINGS

The CC will provide further information on the change management process involved for major changes. The volume and classification of changes will be reviewed during the first few months of operation of the change management process to help to decide the most appropriate frequency of full CC meetings.

The general principle is that all relevant parties are consulted regarding a change that may affect them and these parties may be different according to the scope of a specific change. Therefore, a process of approval via email or telephone may be used in advance of a full CC meeting if the timescale of the change requires a decision before the next meeting.

The relevant parties for the approval of a change will usually be as a minimum:

- User departments affected
- Application support team

Suppliers may also be invited where appropriate.

3.5 CHANGES NOTIFIED BY CLOUD SERVICE PROVIDERS

Changes notified to STEPS by cloud service providers (CSPs) will be assessed by the ICT Department in order to understand and plan for the impact of these changes on the change schedule and on the organization as a whole.

Where appropriate, further information about upcoming changes should be requested from the CSP to allow an accurate impact assessment to be made.

4.0 REPORTING

4.1 REPORTS

The following reports will be produced by the ICT Service Desk System Administrator on a monthly basis and reviewed as part of the ELT meetings in order to identify trends and possible process improvements:

- Number of changes raised and closed by week/month
- Breakdown of categories of change requests raised i.e., Normal, Emergency and Major
- Average time to process a change request of each category
- Percentage successful change requests
- Sources of change requests e.g., business area
- Types of change requests e.g., server, network or by business application

5.0 RELATED DOCUMENTS

Document Name
Nil

6.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	15 April 2021
Effective Date	4 June 2021	**Document Number**	6002400_v1_210603

(Uncontrolled when printed)

1.9.2.8 Information Security Incident Management Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 PURPOSE

This procedure outlines the incident management process including detection, response, and recovery.

2.0 EVENT MANAGEMENT

2.1 INTRODUCTION

An information security event is an occurrence that may indicate that an incident has occurred or is in progress. Effectively, events are clues that need to be assessed to decide if they need further investigation. Most events will probably not result in an incident being raised.

An event is commonly defined as “any change of state that has significance for the management of information security”.

Examples are:

- Notification of a change of an admin password
- Login and logout information at an unusual time
- An unrecognised device having joined the network
- Poor performance of a website
- A device detected as being down when it should be up
- A threshold is breached (or nears being breached) e.g., disk space capacity
- Messages from security software e.g. Host-based intrusion detection systems (HIDS).
- Unauthorised logon attempts to key servers or domains
- Failover devices becoming active.

It is important that events are recognised as potential incidents so that no such clues are missed. Events can occur from many sources, both automated and human and can be of many different types. Often events are captured in logs which are then reviewed to spot any areas for further attention.

2.2 INFORMATION SECURITY EVENT MANAGEMENT PRINCIPLES

In general, the following principles will be adopted regarding the management and assessment of information security events:

- The approach taken to information security event management should be to ensure that business critical services are addressed first
- Event management will attempt to detect potential information security incidents before they occur and prompt appropriate action to be taken so that they are avoided
- The management of events should be centralised as far as possible so that consistency can be achieved in their processing

- Events should be classified as informational, warning or exception and processed according to their classification
- Events that require action to be taken will be logged as incidents and handled according to the Information Security Incident Management Procedure
- Responses to events will be automated where possible to reduce the need for human intervention and minimise support requirements and cost
- All events will be logged and retained in accordance with the relevant record retention policy
- Where possible, appropriate responses to events should be defined in advance and documented. This documentation should be available to support staff at all appropriate times, including out of hours
- Appropriate filtering should be put in place as close to the source of event generation as possible so that events that do not require attention are suppressed and do not use up network capacity
- Where practical, a single event processing engine will be used which is integrated with the incident management system.

Events will occur continuously on most types of devices and software. The process of event management is intended to determine which of these require attention and then to route the event appropriately. Events will be detected via a variety of means, including local software running on the affected device (e.g. Windows event logging) and remote software monitoring devices for certain conditions (e.g. network intrusion detection systems). They may also be recognised by people e.g. employees, suppliers, and customers.

Once an event has been detected it may be assessed automatically by software according to pre-set rules to determine whether it is informational, a warning or an exception. This assessment may take place on a variety of technical platforms in a range of locations (i.e. it is not necessarily centralised). Informational events will be filtered out but may be kept for later analysis. Warning events will be assessed to see if an automated response is required, or it needs to be brought to the attention of the Technology & Cyber Security Manager. Exception events may be escalated from the detecting agent and handled as an incident.

In some cases (particularly for more significant events) the event will then be reviewed to ensure that the correct action has been taken and, if so, it will be closed. This is a general process which will vary widely in its implementation according to the types of devices and software platforms from which events will be generated, however the principles will remain the same. Where possible, monitoring will be localised in order to make use of specialised software appropriate to that device and to minimise network traffic.

In all cases, attention will need to be paid initially and on an ongoing basis to fine tune the suppression, routing, and automation of events on the various platforms so that a useful balance is achieved between maintaining information security and avoiding excessive support requirements. Events recognised by people may be reported to the ICT Service and Support Portal and logged accordingly for review by the information security team.

3.0 PROCEDURE FOR ASSESSING INFORMATION SECURITY EVENTS

The following procedures describes how information security events arise and how they are assessed, either automatically or manually to determine whether they should be treated as incidents.

3.1 EVENT OCCURS

Events will occur in all areas of our infrastructure and applications and may affect the confidentiality, integrity, and availability of many services. STEPS has a wide range of technology platforms, networks, and systems from many vendors, each of which has its own techniques and conventions for generating events related to information security.

Effective planning and design will help to reduce the number of exception and warning events that are generated, and informational events will be restricted to those that assist in the management of information security. Excessive generation of events that are not required for warning, exception or audit purposes will be avoided and systems configured as such.

3.2 AUTOMATED EVENT OCCURS

Once an automated event has occurred it will be communicated to the associated monitoring software. In some cases, this will be a module within the system that has generated the event, or it may be an agent running on the same platform or a remote monitoring tool that performs information security “health checks” on a regular basis.

3.3 EVENT LOGGED

The event will be logged in order to act as an original record of the event that occurred. This may take place in several places, for example where an event is logged on a local system and then the record is also forwarded to a central monitoring point. This is particularly relevant in security breach situations where the remote log may be taken as more trustworthy than the original which is on the compromised system.

Events will be reported in the ICT Security Incident form found in the ICT Service & Support Portal.

3.4 FIRST-LEVEL EVENT CORRELATION AND FILTERING

The event will then be assessed to determine its type, which may be one of:

- Informational – no action is necessary
- Warning – action may be required soon, or now to prevent an exception
- Exception – action is required to address an out of line situation.

This assessment may be carried out automatically in several locations according to the way in which the component generating the event is monitored. For components that have built in event logging the first-level event correlation will take place on the device itself. For devices monitored remotely it is likely to happen on the remote monitoring system.

Where possible, events generated automatically will give a standard indication of their severity i.e., whether they are informational, warnings or exceptions. This standard will be defined and used in all areas in which messages can be tailored to comply with it and will include:

- Message type – informational, warning, exception
- Impact and urgency of the event
- Event description in terms understandable by the intended recipient
- Normal resolution actions if appropriate
- Escalation information.

3.5 INFORMATION EVENTS

Informational events will be automatically closed (although this may not involve any explicit action) and kept for a period according to the record retention policy. Although not forwarded, informational events may still be required for operational purposes to provide an audit trail as part of later investigations.

3.6 WARNING EVENTS

Those events that are classified as warnings will be subject to further review. Ideally this will be automated via a correlation engine, but this may also be a manual activity carried out by ICT staff.

If it is determined that no further action is required at the time, the event will be closed. For those events that need action to be taken, an automated response may be triggered by the correlation engine e.g., to increase table size in a database. If an automated response is not possible then a member of the support team will need to decide about what to do next. The information contained in the event message may help in deciding this.

If appropriate, the warning message may be automatically escalated to support staff. This may often be the case if the event occurs outside of normal support hours when an on-call person may need to be emailed, SMS/text or contacted via some other means. The individual contacted will then decide upon further action to be taken.

3.7 EXCEPTION EVENTS

For events that are deemed to be exceptions, an incident will be raised, and the event will then be managed via the Information Security Incident Management Procedure with appropriate diagnosis, investigation, and escalation. This may be done automatically or manually.

Key considerations in deciding whether an event represents an incident will include situations where:

- there is evidence of deliberate human interaction for malicious purposes
- the information involved is of a high classification level
- the circumstances are unusual in some way
- there is a clear breach of Information Security Policy

- there is obvious potential for the situation to worsen if not addressed
- the actual or potential impact on the organisation is significant
- there is evidence of a control not working effectively
- a set of behaviours known to be malicious is displayed
- there is any other reason to be suspicious.

If there is doubt about whether an information security incident should be raised, employees should err on the side of caution. Such situations should then be reviewed after the completion of investigations to decide whether similar events in the future should be raised as incidents.

3.8 REVIEW ACTIONS

For those events that are more significant (i.e. they have a bigger impact on services) a review will be undertaken to ensure that the process has worked effectively and that all required actions have been taken. If this is found not to be the case, a repeat of earlier activities in the procedure may be needed.

3.9 CLOSE EVENT

If the event has been handled satisfactorily it is then closed. Exception events that result in an incident being raised will be subject to the Incident Management Procedure (i090000) and may be closed under the control of that procedure.

4.0 INCIDENT RESPONSE

4.1 INTRODUCTION

This section is intended to be used when an incident of some kind has occurred that affects the information security of STEPS. It is intended to ensure a quick, effective, and orderly response to information security incidents.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

- provide a concise overview of how STEPS will respond to an incident affecting its information security
- set out who will respond to an incident and their roles and responsibilities
- describe the facilities that are in place to help with the management of the incident
- define how decisions will be taken about our response to an incident

- explain how communication within the organization and with external parties will be handled
- provide contact details for key people and external agencies
- define what will happen once the incident is resolved and finalise.

Contact details will be checked and updated at least six-monthly. Changes to contact or other relevant details that occur outside of these scheduled checks should be sent to ICT Service and Support Portal as soon as possible after the change has occurred.

4.2 INCIDENT DETECTION AND ANALYSIS

The incident may be initially detected in a wide variety of ways and through several different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within STEPS or by employees noticing unusual activity (see the Information Security Event Assessment section for details of how events are assessed). Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of the Information Security Management System (ISMS) is to reduce this time period. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

Once the incident has been detected, an initial impact assessment must be carried out in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on ICT infrastructure including computers, networks, equipment
- The information assets that may be at risk or have been compromised
- The likely duration of the incident i.e., when it may have begun
- The business units affected and the extent of the impact to them
- Initial indication of the likely cause of the incident.

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets, business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

As a result of this initial analysis, any member of the Executive Managers has the authority to contact the Incident Response Team Leader at any time to ask him/her to assess whether the Incident Response process should be activated.

4.3 ACTIVATING THE INCIDENT RESPONSE PROCEDURE

Once notified of an incident the Technology & Cyber Security Manager (or delegate) must decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response process and the convening of the Incident Response Team (IRT).

Guidelines for whether a formal incident response should be initiated for any incident of which the Technology & Cyber Security Manager (or delegate) has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact to the organisation.

If it is decided not to activate the procedure, then a plan should be created to allow for a lower-level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

If the incident warrants the activation of the Incident Response process the Technology & Cyber Security Manager (or delegate) will start to assemble the Incident Response Team.

4.4 ASSEMBLE INCIDENT RESPONSE TEAM

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) will ensure that all role holders (or their deputies if main role holders are un-contactable) are contacted, made aware of the nature of the incident, and asked to assemble at an appropriate location.

The exception is the Incident Liaison who will be asked to attend the location of the incident (if different) in order to start to gather information for the incident assessment that the IRT will conduct so that an appropriate response can be determined. Assemble Incident Response Team

The Incident Response Team will generally consist of the following people in the roles specified and with the stated deputies, although the exact make-up of the team will vary according to the nature of the incident.

Role/Business Area	Main role holder	Deputy
Team Leader	Technology & Cyber Security Manager	Cyber Security & Systems Engineer
Team Facilitator	Chief Administrative Officer	Manager – Executive Administration
Incident Liaison	Business Manager	Business Manager
Information Technology	Technology & Cyber Security Manager	Cyber Security & Systems Engineer

Business Operations	Chief Operating Officer	Chief Administrative Officer
Facilities Management	Managing Director	Asset Manager
Health and Safety	Executive Manager – Human Resources	Workplace Health and Safety Officer – Human Resources
Human Resources	Executive Manager – Human Resources	HR Operations Manager
ICT Business Continuity Planning	Chief Administrative Officer	Technology & Cyber Security Manager
Communications (PR and Media Relations)	Managing Director	Customer Success Manager
Legal and Regulatory	Managing Director	Chief Operating Officer

Table 1 – Incident response team members

4.5 ROLES AND RESPONSIBILITIES

The responsibilities of the roles within the incident response team are as follows:

Team Leader

- Decides whether to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the Managing Director and other high-level stakeholders.

Team Facilitator

- Supports the incident response team
- Coordinates resources within the command centre
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the command centre
- Facilitates communication via email, SMS/text, telephone, or other methods
- Monitors external information feeds such as news.

Incident Liaison

- Attends the site of the incident as quickly as possible
- Assesses the extent and impact of the incident
- Provides first-person account of the situation to the IRT
- Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT.

Information Technology

- Provides input on technology-related issues
- Assists with impact assessment.

Business Operations

- Contributes to decision-making based on knowledge of business operations, products, and services
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organisation.

Facilities Management

- Deals with aspects of physical security and access
- Provides security presence if required.

Health and Safety

- Assesses the risk to life and limb of the incident
- Ensures that legal responsibilities for health and safety are always met
- Liaises with emergency services such as police, fire and medical
- Considers environmental issues with respect to the incident.

Human Resources

- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organisation employees
- Advises on capability and disciplinary issues.

Business Continuity Planning

- Provide advice on business continuity options
- Invoke business continuity plans if required.

Communications (PR and Media Relations)

- Responsible for ensuring internal communications are effective
- Decides the level, frequency, and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed e.g., customers, shareholders.

Legal and Regulatory

- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks.
- Assesses the actual and potential legal implications of the incident and subsequent actions.

5.0 INCIDENT MANAGEMENT, MONITORING AND COMMUNICATION

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings must be held at an appropriate frequency decided by the Team Leader. A standard agenda for these meeting is defined below:

Attendees: All members of Incident Response Team

Frequency: Every Hours / Days

Chair: Team Leader

Minutes: Team Facilitator

1. Actions from previous meeting
2. Incident status update
3. Decisions required
4. Task allocation
5. Internal communications
6. External communications
7. Finalisation
8. Any other business

The purpose of these meetings is to ensure that incident management resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be documented by the Team Facilitator (or delegate).

The Incident Liaison will provide updates to the IRT to a frequency decided by the Team Leader. These updates should be coordinated with the IRT meetings so that the latest information is available for each meeting.

5.1 COMMUNICATION PROCEDURE

It is vital that effective communications are maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face and telephone, either landline or mobile. Email should not be used unless permission to do so has been given by the IRT.

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation
- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
    - Ask if the contact is available elsewhere
    - If they cannot be contacted leave a message to contact, you on a given number
    - Do not provide details of the Incident.
- Always document call time details, responses, and actions

All communications should be clearly and accurately recorded as records may be needed as part of legal action later.

5.2 EXTERNAL COMMUNICATION

Depending on the incident there may be a variety of external parties that will be communicated with during the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

There may be several external parties who, whilst not directly involved in the incident, may be affected by it, and need to be alerted to this fact. These may include:

- Customers
- Suppliers
- Stakeholders
- Regulatory bodies.

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of IRT.

5.3 COMMUNICATION WITH THE MEDIA

In general, the communication strategy with respect to the media will be to issue updates via the Managing Director and the Executive Leadership Team (ELT). No members of staff should give an interview with the media.

The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

In drafting a statement for the media, the following guidelines should be observed:

- Personal information should be always protected
- Stick to the facts and do not speculate about the incident or its cause
- Ensure legal advice is obtained prior to any statements being issue.
- Try to pre-empt questions that may reasonably be asked
- Emphasise that a prepared response has been activated and that everything possible is being done.

6. INCIDENT CONTAINMENT, ERADICATION, RECOVERY AND NOTIFICATION

6.1 CONTAINMENT

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting the affected parts of the network; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: If it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident e.g. by waking up a laptop. It is recommended that specialist advice be obtained at this point.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1 – Don't change any data. If anything is done that results in the data on the relevant system being altered in any way, then this will affect any subsequent court case.

Principle 2 – Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g., time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically, but this also applies to the first people on the scene. Taking photographs and videos is encouraged if nothing is touched to do it.

Principle 4 – The person in charge must ensure that the guidelines are followed.

Prior to the arrival of a specialist basic information should be collected.

This may include:

- Photographs or videos of relevant messages or information
- Manual written records of the chronology of the incident
- Original documents, including records of who found them, where and when
- Details of any witnesses.

Once collected, the evidence will be kept in a safe place where it cannot be tampered with, and a formal chain of custody established.

The evidence may be required:

- For later analysis as to the cause of the incident.
- As forensic evidence for criminal or civil court proceedings.
- In support of any compensation negotiations with software or service suppliers.

Next, a clear picture of what has happened needs to be established. The extent of the incident and the knock-on implications should be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

6.2 ERADICATION

Actions to fix the damage caused by the incident, such as deleting malware, must be put through the change management process (as an emergency change if necessary). These actions should be aimed at fixing the current cause and preventing the incident from reoccurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

6.3 RECOVERY

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers, and amending procedures.

6.4 NOTIFICATION

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

6.5 BREACH NOTIFICATION

Refer to the Data Breach Identification and Reporting Procedure (i020500).

7.0 FINALISATION

All actions taken as part of incident response should be recorded. The Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident.

Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident.

8.0 RELATED DOCUMENTS

Document Name	Document Name
Business Continuity Plan (i100104)	Data Breach Identification and Reporting Procedure (i020500)
ICT Incident Security Form (ICT Service & Support Portal)	Incident Management Procedure (i090000)
Information Security Policy (6002300)	WHS Incident Report (i090201)

9.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023

Effective Date	1 June 2023	**Document Number**	6000600_v2_230601

(Uncontrolled when printed)

1.9.2.9 Network Access and Authentication Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as "STEPS".

1.1 Definitions

Antivirus Software	An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
Authentication	A security method used to verify the identity of a user and authorise access to a system or network.
Biometrics	The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.
Encryption	The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
Password	A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.
Smart Card	A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.
Token	A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

2.0 PROCEDURE

2.1 ACCOUNT SETUP

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following are required for account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted least amount of network access required to perform his or her job function.
- Users will be granted access only if he or she accepts the Acceptable Use Policy (6001700).
- Access to the network will be granted in accordance with the Acceptable Use Policy (6001700).

2.2 ACCOUNT USE

Network accounts must be implemented in a standard fashion and utilised consistently across the organisation. The following requirements apply to account use:

- Accounts must be created using a standard format (i.e. firstname firstinitial lastname).
- Accounts must be password protected (refer to the Password Procedure (6001100) for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- User accounts must not be given administrator or 'root' access.
- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.
- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the Technical & Cyber Security Manager or Executive Leadership team, or as required by applicable regulations or third-party agreements.

2.3 ACCOUNT TERMINATION

In the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.), the Human Resources department will notify the ICT Department at the soonest possible time to allow for the employee’s account to be disabled or altered in line with the changed status of the employee.

2.4 AUTHENTICATION

User machines must be configured to request authentication against the domain at startup.

2.5 USE OF PASSWORDS

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to STEPS' Password Procedure (6001100).

2.6 REMOTE NETWORK ACCESS

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, STEPS encourages additional scrutiny of users remotely accessing the network. STEPS' standards dictate that username and password is an acceptable means of authentication if appropriate policies are followed. Remote access must adhere to the VPN Procedure (6001500).

2.7 SLEEP AND AWAKEN PASSWORDS

Passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, sleep and awaken passwords are implemented.

2.8 MINIMUM CONFIGURATION FOR ACCESS

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards about antivirus software and patch levels on their machines. When discovered, users will not be permitted network access if these standards are not met.

2.9 ENCRYPTION

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to STEPS network or across a public network such as the Internet.

2.10 FAILED LOGONS

To protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

2.11 NON-BUSINESS HOURS

While some security can be gained by removing account access capabilities during non-business hours, STEPS does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because STEPS' business requires all-hours access.

2.12 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name	Document Name

Acceptable Use Policy (6001700)	Password Procedure (6001100)
VPN Procedure (6001500)	

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6000800_v2_230601

(Uncontrolled when printed)

(Uncontrolled when printed)

1.9.2.10 Network Security Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 DEFINITIONS

ACL	Stands for Access Control List. A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.
Antivirus Software	An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
Firewall	A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.
IDS	Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.
IPS	Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

NTP	Stands for Network Time Protocol. A protocol used to synchronise the clocks on networked devices.
Password	A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
RAID	Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.
Switch	A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.
VLAN	Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.
Virus	Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files like how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

2.0 PROCEDURE

2.1 NETWORK DEVICE PASSWORDS

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

2.2 PASSWORD CONSTRUCTION

The following statements apply to the construction of passwords for network devices:

- Passwords should be at least 14 characters.
- Passwords should not be comprised of, or otherwise utilise, words that can be found in a dictionary.
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty).
- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

2.3 FAILED LOGONS

To protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

2.4 CHANGE REQUIREMENTS

Passwords must be changed according to STEPS' Password Procedure (6001100). Additionally, the following requirements apply to changing network device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
- If a company network or system administrator leaves STEPS, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.
- Vendor default passwords must be changed when new devices are put into service.

2.5 PASSWORD PROCEDURE ENFORCEMENT

If possible, where passwords are used an application should be implemented that enforces STEPS' password policies on construction, changes, re-use, lockout, etc.

2.6 ADMINISTRATIVE PASSWORD GUIDELINES

As a rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

2.7 LOGGING

The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail STEPS' requirements for logging and log review.

2.8 APPLICATION AND FILE SERVERS

Logs from application and file servers are of interest since these servers often allow connections from many internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, file server, database servers.

Logging of at least errors, faults, and login failures is achieved using standard log monitoring software. No passwords should be contained in logs.

2.9 NETWORK DEVICES

Logs from network devices are of interest since these devices control all network traffic and can have a huge impact on STEPS' security.

Examples: Firewalls, network switches, routers

Darktrace has been implemented to analyse logs from network devices and report on events that need to be reviewed by the ICT Team.

2.10 LOG MANAGEMENT

While logging is important to STEPS' network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, a standard log management tool has been implemented.

2.11 LOG REVIEW

Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events which are then reviewed by a member of the ICT team. Any security events that need to be escalated and reviewed are brought to the attention of the Cyber

Security and Systems Engineer and Technology & Cyber Security Manager in accordance with the Information Security Incident Management Procedure (6000600).

2.12 LOG RETENTION

Logs should be retained in accordance with STEPS' Records Management Procedure (i020300). Unless otherwise determined by the Technology & Cyber Security Manager, logs should be considered restricted data as per the Data Classification Procedure (6000300).

2.13 FIREWALLS

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks are separated from STEPS network using a firewall provided by Vocus and Darktrace network monitoring.

2.14 CONFIGURATION

The following statements apply to STEPS' implementation of firewall technology:

- Firewalls must provide secure administrative access (using encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- No unnecessary services or applications are enabled on firewalls. STEPS uses 'hardened' systems for firewall platforms, or appliances.
- Clocks on firewalls are synchronised with STEPS' other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- For its own protection, the firewall ruleset should include a "stealth rule," which forbids connections to the firewall itself.
- The firewall should log, dropped or rejected packets.

2.15 OUTBOUND TRAFFIC FILTERING

STEPS requires that permitted outbound traffic be limited to only known "good" services, which are the following ports: 21, 22, 23, 25, 53, 80, 110, 443, and 995. All other outbound traffic is blocked at the firewall unless an exception is granted from the Technology and Cyber Security Manager.

2.16 NETWORKING HARDWARE

Networking hardware, such as routers, switches, and access points, should be implemented in a consistent manner. The following statements apply to STEPS' implementation of networking hardware:

- Networking hardware must provide secure administrative access (using encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- Clocks on all network hardware should be synchronised using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- If possible, for the application, switches are preferred over hubs. When using switches STEPS should use VLANs to separate networks if it is reasonable and possible to do so.
- Access control lists should be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.

- Unused services and ports should be disabled on networking hardware.
- Access to administrative ports on networking hardware should be restricted to known management hosts and otherwise blocked with a firewall or access control list.

2.17 NETWORK SERVERS

Servers typically accept connections from several sources, both internal and external. As a rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to STEPS' use of network servers:

- Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
- A standard installation process is used for STEPS' network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.
- Clocks on network servers should be synchronised with STEPS' other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

2.18 INTRUSION DETECTION/INTRUSION PREVENTION

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology has been implemented using Darktrace. The alerts and events generated by the system are monitored by the ICT Team and managed in accordance with the Information Security Incident Management Procedure (6000600).

2.19 SECURITY TESTING

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining STEPS' network security. Security testing can be provided by ICT Staff members but is often more effective when performed by a third party with no connection to STEPS' day-to-day Information Technology activities. The following sections detail STEPS' requirements for security testing.

2.20 EXTERNAL SECURITY TESTING

External security testing, which is testing by a third-party entity, is an excellent way to audit STEPS' security controls. The Technology & Cyber Security Manager determines to what extent this testing should be performed, and what systems/applications it should cover.

External testing must not negatively affect network performance during business hours or network security at any time.

As a rule, "penetration testing," which is the active exploitation of company vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact company systems or data.

STEPS encourages external security testing but does not provide rigid guidelines regarding at what intervals the testing should occur. Testing should be performed as often as is necessary, as determined by the Technology & Cyber Security Manager.

2.21 DISPOSAL OF INFORMATION TECHNOLOGY ASSETS

ICT assets, such as network servers and routers, often contain sensitive data about STEPS' network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify STEPS must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
- At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, STEPS must use the most secure commercially available methods for data wiping. Alternatively, STEPS has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid-state memory).

2.22 NETWORK COMPARTMENTALISATION

Good network design is integral to network security. By implementing network compartmentalisation, which is separating the network into different segments, STEPS will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. STEPS requires the following about network compartmentalisation:

2.23 HIGHER RISK NETWORKS

Examples: Guest network, wireless network.

Guest networks and wireless networks have been segregated from the STEPS corporate networks.

2.24 EXTERNALLY ACCESSIBLE SYSTEMS

Examples: Email servers, web servers

Externally accessible systems have been segregated from STEPS internal networks.

2.25 INTERNAL NETWORKS

Examples: Sales, Finance, Human Resources

Segmentation of internal networks has been conducted based on risk as determined by the Technology & Cyber Security Manager.

2.26 NETWORK DOCUMENTATION

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that STEPS' ICT Staff has a firm understanding of the network architecture at any given time.

The network documentation includes:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses.

2.27 ANTIVIRUS/ANTI-MALWARE

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire company. STEPS provides the following guidelines on the use of antivirus/anti-malware software:

- All company-provided user workstations must have antivirus/anti-malware software installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.
- In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.

2.28 SOFTWARE USE PROCEDURE

Software applications can create risk in several ways, and thus certain aspects of software use must be covered by this procedure. STEPS provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for STEPS' software must be stored in a secure location.
- Open source and/or public domain software can only be used with the permission of the Technology & Cyber Security Manager.
- Software should be kept reasonably up to date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that STEPS uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

2.29 MAINTENANCE WINDOWS AND SCHEDULED DOWNTIME

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the ICT Staff should make every effort to perform the tasks at times when they will have the least impact on network users.

2.30 CHANGE MANAGEMENT

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The ICT Staff should make a reasonable effort to document hardware and/or configuration changes to network devices in a "change log." If possible, network devices should bear a sticker or tag indicating essential information, such as the device name, IP address, Mac address, asset information, and any additional data that may be helpful, such as information about cabling.

2.31 REDUNDANCY

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. STEPS wishes to provide the Technology & Cyber Security Manager with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability

- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite

2.32 MANUFACTURER SUPPORT CONTRACTS

Outdated products can result in a serious security breach. When purchasing critical hardware or software, STEPS should purchase a maintenance plan, support agreement, or software subscription that will allow STEPS to receive updates to the software and/or firmware for a specified period. The plan must meet the following minimum requirements:

Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time, as determined by the Technology & Cyber Security Manager, as well as firmware or embedded software updates.

Software: The arrangement must allow for updates, upgrades and hotfixes for a specified period.

2.33 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Data Classification Procedure (6000300)	Information Security Incident Management Procedure (6000600)
Password Procedure (6001100)	Records Management Archiving Procedure (i020300)

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6000900_v2_230601

(Uncontrolled when printed)

1.9.2.11 Outsourcing Procedure

1.0 INTRODUCTION

1.0 DEFINITIONS

Backup	To copy data to a second location, solely for the purpose of safe keeping of that data.
Encryption	The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
Network Management	A far-reaching term that refers to the process of maintaining and administering a network to ensure its availability, performance, and security.
Remote Access	The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.
Virtual Private Network (VPN)	A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

2.0 PROCEDURE

2.1 DECIDING TO OUTSOURCE

Outsourcing services is often necessary but should be carefully considered, since by nature a certain amount of control will be lost by doing so. The following questions must be affirmatively answered before outsourcing is considered:

- Can the service be performed better or less expensively by a third-party provider?
- Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house?
- Will outsourcing the service positively affect the quality of this service?
- Is the cost of this service worth the benefit?
- Are any risks associated with outsourcing the service worth the benefit?
- Is there a strategic reason to have the service in-house?

2.2 OUTSOURCING CORE FUNCTIONS

STEPS permits the outsourcing of critical and/or core functions of STEPS' processes if this procedure, in conjunction with ICT Change Management Procedure (6002400), is followed.

2.3 EVALUATING A PROVIDER

Once the decision to outsource a function has been made, selecting the appropriate provider is critical to the success of the endeavour. Due diligence must be performed after the potential providers have been pared to a short list of two to three companies. Due diligence must always be performed prior to a provider being selected.

Due diligence must include an evaluation of the provider's ability to perform the requested services and meet STEPS' security requirement, the Non-Functional Requirements Checklist (6000003) must be completed by the approved manager with a copy provided to the Technology & Cyber Security Manager and Chief Financial Officer (CFO). It should involve a review of the provider's reputation, technical ability, and experience providing the same services to similar companies.

If the outsourced service will involve the provider having access to, or storing STEPS' confidential information, due diligence should cover the provider's security controls for access to the confidential information.

2.4 SECURITY CONTROLS

The outsourcing contract must provide a mechanism for secure information exchange with the service provider. This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange.

STEPS and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to company data.

2.5 OUTSOURCING CONTRACTS

All outsourced services must be governed by a legal contract, with an original of the executed contract maintained by STEPS. Contracts must:

- Cover a specified time period
- Specify exact pricing for the services
- Specify how the provider will treat confidential information
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for missing the levels
- Agree security controls and incident reporting requirements
- Allow for cancellation if contractual terms are not met
- Specify standards for subcontracting of the services and reassignment of contract
- Cover liability issues
- Describe how and where to handle contractual disputes
- Exit processes to enable business continuity.

2.6 ACCESS TO INFORMATION

The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable procedures and be periodically audited.

2.7 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name	Document Name
ICT Change Management Procedure (6002400)	Non-Functional Requirements Checklist (6000003)

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	17 January 2024
Effective Date	11 June 2024	**Document Number**	6001000_v3_240611

(Uncontrolled when printed)

1.9.2.12 Password Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS”.

1.1 DEFINITIONS

Authentication	A security method used to verify the identity of a user and authorise access to a system or network.
Password	A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
Multi-Factor Authentication	A means of authenticating a user that utilises two methods: something the user has, and something the user knows. Examples are PIN, smart cards, tokens, or biometrics, in combination with a password.

Single-Factor Authentication	A means of authenticating a user that utilises one method: something the user knows. Examples are passwords, PIN, pattern.

2.0 PROCEDURE

2.1 CONSTRUCTION

The best security against a password incident is simple: following a sound password construction strategy. The organisation mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 10 characters when used with Multi-Factor Authentication or 14 characters when used as Single-Factor Authentication.
- Passwords should be comprised of a unique passphrase.
- Passwords should not be comprised of, or otherwise utilise, words that can be found in a dictionary.
- Passwords should not be comprised of an obvious keyboard sequence (i.e. qwerty).
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

A way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Procedure (6001100), but this technique will help make strong passwords easier for users to remember.

2.2 CONFIDENTIALITY

Passwords should be considered confidential data and treated with the same discretion as any of the organisation's proprietary information. The following guidelines apply to the confidentiality of passwords:

- Users must not disclose their passwords to anyone, nor should users request passwords from other users
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured.
- Users must not check the "save password" box when authenticating to applications
- Users must not use the same password for different systems and/or account.
- Users must not send passwords via email
- Users must not re-use passwords.

2.3 CHANGE FREQUENCY

To maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. The organisation will use software that enforces this procedure by expiring users' passwords every twelve months.

2.4 INCIDENT REPORTING

Since compromise of a single password can have a catastrophic impact on network security, it is the user’s responsibility to immediately report any suspicious activity involving his or her passwords to the Technology & Cyber Security Manager. Any request for passwords over the phone or email, whether the request came from organisation personnel or not, should be expediently reported. When a password is suspected to have been compromised the Technology & Cyber Security Manager will request that the user, or users, change all his or her passwords.

2.5 APPLICABILITY OF OTHER PROCEDURES

This document is part of the organisation's cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager on behalf of the Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name
Nil

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	24 June 2024
Effective Date	5 July 2024	**Document Number**	6001100_v3_240705

(Uncontrolled when printed)

1.9.2.13 Physical Security Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 DEFINITIONS

Biometrics	The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, facial recognition, and hand geometry.
Datacenter	A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.
Key Card	A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.
Keypad	A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.
Mobile Device	A portable device that can be used for certain applications and data storage. Examples are laptops or Smartphones.
PDA	Stands for Personal Digital Assistant. A portable device that stores and organises personal information, such as contact information, calendar, and notes.
Smartphone	A mobile telephone that offers additional applications, such as PDA functions and email.
Uninterruptible Power Supplies (UPSs)	A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

2.0 PROCEDURE

2.1 CHOOSING A SITE

When possible, thought should be given to selecting a site that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacenter or a site for centralised ICT operations. At a minimum, STEPS' site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters
- A site should not be in an area where the crime rate and/or risk of theft is higher than average
- A site should have the fewest number of entry points possible.

2.2 SECURITY ZONES

At a minimum, STEPS will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure STEPS' assets. In addition to this STEPS must provide security in layers by designating different security zones within the building. Security zones should include:

Public This includes areas of the building or office that are intended for public access.

- Access Restrictions: None

- Additional Security Controls: None
- Examples: Lobby, common areas of building

Company This includes areas of the building or office that are used only by employees and other persons for official company business.

- Access Restrictions: Only company personnel and approved/escorted guests
- Additional Security Controls: None
- Examples: Hallways, private offices, work areas, conference rooms

Private This includes areas that are restricted to use by certain persons within STEPS, such as executives, and ICT personnel, for security or safety reasons.

- Access Restrictions: Only specifically approved personnel
- Additional Security Controls: None
- Examples: Executive offices, server room, HR offices, financial offices, and storage areas.

2.3 ACCESS CONTROLS

Access controls are necessary to restrict entry to STEPS premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with STEPS' guidelines for their use.

2.4 KEYS & KEYPADS

The use of keys and keypads is acceptable. These security mechanisms are the most inexpensive and is the most familiar to users. The disadvantage is that STEPS has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied, and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good security can be obtained with keys and keypads.

2.5 KEY CARDS

While keycards are allowable forms of access controls, STEPS do not currently require their use.

Keycards have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorised. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled.

2.6 ALARM SYSTEM

A security alarm system is a good way to minimise risk of theft or reduce loss in the event of a theft.

2.7 PHYSICAL DATA SECURITY

Certain physical precautions must be taken to ensure the integrity of STEPS' data. At a minimum, the following guidelines must be followed:

- Wherever possible computer screens should be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information should not be displayed on a computer screen where the screen can be viewed by those not authorised to view the information.

- Users must log off or shut down their workstations when leaving for an extended time, or at the end of the workday.
- Network cabling should not run through unsecured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
- STEPS recommends disabling network ports that are not in use.

2.8 PHYSICAL SYSTEM SECURITY

In addition to protecting the data on STEPS' information technology assets, this procedure provides the guidelines below on keeping the systems themselves secure from damage or theft.

2.9 MINIMISING RISK OF LOSS AND THEFT

To minimise the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- **Unused systems:** If a system is not in use for an extended period it should be moved to a secure area or otherwise secured.
- **Mobile devices:** Special precautions must be taken to prevent loss or theft of mobile devices. Refer to STEPS' Mobile Device Policy (6002100) for guidance.
- **Systems that store confidential data:** Special precautions must be taken to prevent loss or theft of these systems. Refer to STEPS' Confidential Data Procedure (6000200) for guidance.

2.10 MINIMISING RISK OF DAMAGE

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. To minimise the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimised.
- Strong magnets must not be used in proximity to company systems or media.
- Except in the case of a fire suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto company systems.
- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems.

2.11 FIRE PREVENTION

It is STEPS' procedure to provide a safe workplace that minimises the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of ICT systems, the fire danger in these areas is typically higher than other areas of STEPS' office. The guidelines below are intended to be specific to STEPS' information technology assets and should conform to STEPS' overall fire safety procedure.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if practical.
- Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.
- A smoke alarm monitoring service should be considered that will alert a designated company employee if an alarm is tripped during non-business hours.

2.12 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Confidential Data Procedure (6000200)	Mobile Device Policy (6002100)

4.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6001200_v2_230601

(Uncontrolled when printed)

1.9.2.14 Risk Management Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 PURPOSE

Information assets are key enablers to achieve the business objectives for STEPS. These information assets should be adequately protected from various threats that could lead to compromise of their Confidentiality, Integrity and Availability.

The purpose of this document is to present a risk assessment process, that is designed to systematically identify, analyse, and evaluate the information security risks associated with the loss of Confidentiality, Integrity, and Availability of information within the scope of the STEPS’ information security management system (hereafter, referred to as ISMS).

The risk assessment process defined in this document is built on an asset-based approach in order to meet ISO 27001:2013 (Section 6.1.2 & 6.1.3) requirements. This process should be followed as an ongoing activity to maintain ISO 27001:2013 certification.

1.2 SCOPE

The scope of this document is limited to all information assets that fall within the scope of STEPS’ ISMS. *Refer to ISMS Scope (6000005) section in the ISMS Manual (6000004).*

1.3 DEFINITIONS

Context	Defining the external and internal parameters to be taken into account when managing risk.
Risk	The effect of uncertainty on objectives, often expressed in terms of a combination of the consequences of an event, including changes in circumstances, and the associated likelihood of occurrence.
Opportunity	The potential beneficial effects, often expressed as a situation or condition that is favourable for the attainment of a goal or advancement for success.
Risk Assessment	Coordinated activities to direct and control an organisation regarding risk. The overall process includes risk identification (threats and vulnerabilities), risk analysis and risk evaluation.
Risk Treatment	Involves developing a range of options for mitigating the risk, assessing those options, and then preparing and implementing action plans.
Confidentiality	Confidentiality is the property, that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Integrity	Integrity is maintaining and assuring the accuracy and completeness of information over its entire life-cycle.

Availability	Property of being accessible and usable upon demand by an authorised entity
Risk Owner	Person or entity with accountability and authority to manage a risk

1.4 RESPONSIBILITIES

Position	Responsibilities
Executive Leadership Team	• Provide adequate resources to assist with the implementation of the procedure • Ensure that staff are adequately trained to follow this procedure • Ensure that staff are following this procedure for all projects
Chief Administrative Officer	• Maintain the *Information Security Risk Register* and ensure that corporate risks, opportunities, and information security risks are added
Risk Owner	The Risk Owner is the person or entity with accountability and authority to manage a risk including: • Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity, and availability of STEPS information assets • Approve information security risk treatment plans and accept the residual information security risks
Asset Owner	For corporate information, the designated Asset Owner has the authority to make decisions related to the development, maintenance, operation of and access to the application and data belonging to the information asset. • Interpreting pertinent standards, laws, and STEPS policies to classify information to define the level of confidentiality, integrity, and availability required. • Defining required levels of security, including those for data transmission. • Developing guidelines for data and/or information access. • Reviewing and authorising (delegating authority) for access requests.

	• Defining criteria for archiving data and information, to satisfy retention requirements. • Assigning day-to-day administrative and operational responsibilities for STEPS information assets to one or more Asset Custodians. • Require Asset Custodians to implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of STEPS information assets
Asset Custodian	An Asset Custodian is an employee of STEPS who has administrative and/or operational responsibility over a STEPS information asset. In many cases, there will be multiple Asset Custodians. An enterprise application may have teams of Asset Custodians, each responsible for varying functions. An Asset Custodian is responsible for the following: • Understanding and reporting on how STEPS information is stored, processed, and transmitted by STEPS and by third-party Agents of STEPS. • Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of STEPS information assets • Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing, and transmission of STEPS information assets. • Provisioning and deprovisioning access to STEPS information assets as authorised by the Asset Owner. • Understanding and reporting on security risks and how they impact the confidentiality, integrity, and availability of STEPS information assets. • Ensure that employees, contractors, Board members, and third-party providers understand their responsibilities and where applicable, STEPS' security policies and procedures
Employees	• Assist with identifying risks, assessing them, and assigning treatment options • Report any issues to the Asset Owner

2.0 RISK ASSESSMENT PROCESS OVERVIEW

Organisations operating today have an increasing reliance on their information and ICT Systems in order to achieve their business goals and objectives. An effective risk assessment process is an important component of a successful information security program.

Risk management is the process of identifying, controlling, and mitigating information system–related risks. It involves the process of identifying threats and vulnerabilities to information assets and deciding the countermeasures that need to be taken to bring the risk to an acceptable level.

The process detailed in this document is aligned with and based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2018 risk management standards. Figure 1 below presents the risk management lifecycle as defined in AS/NZS ISO 31000 of which risk assessment is one aspect.

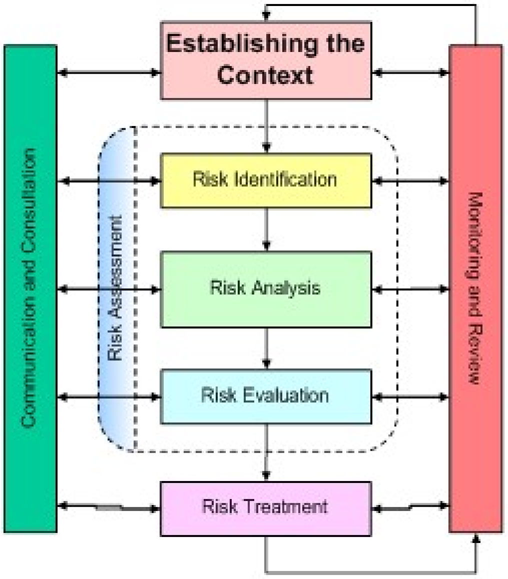


Figure 1: - Risk Management Lifecycle

2.1 RISK ASSESSMENT STEPS

The diagram below illustrates the information security risk management process.

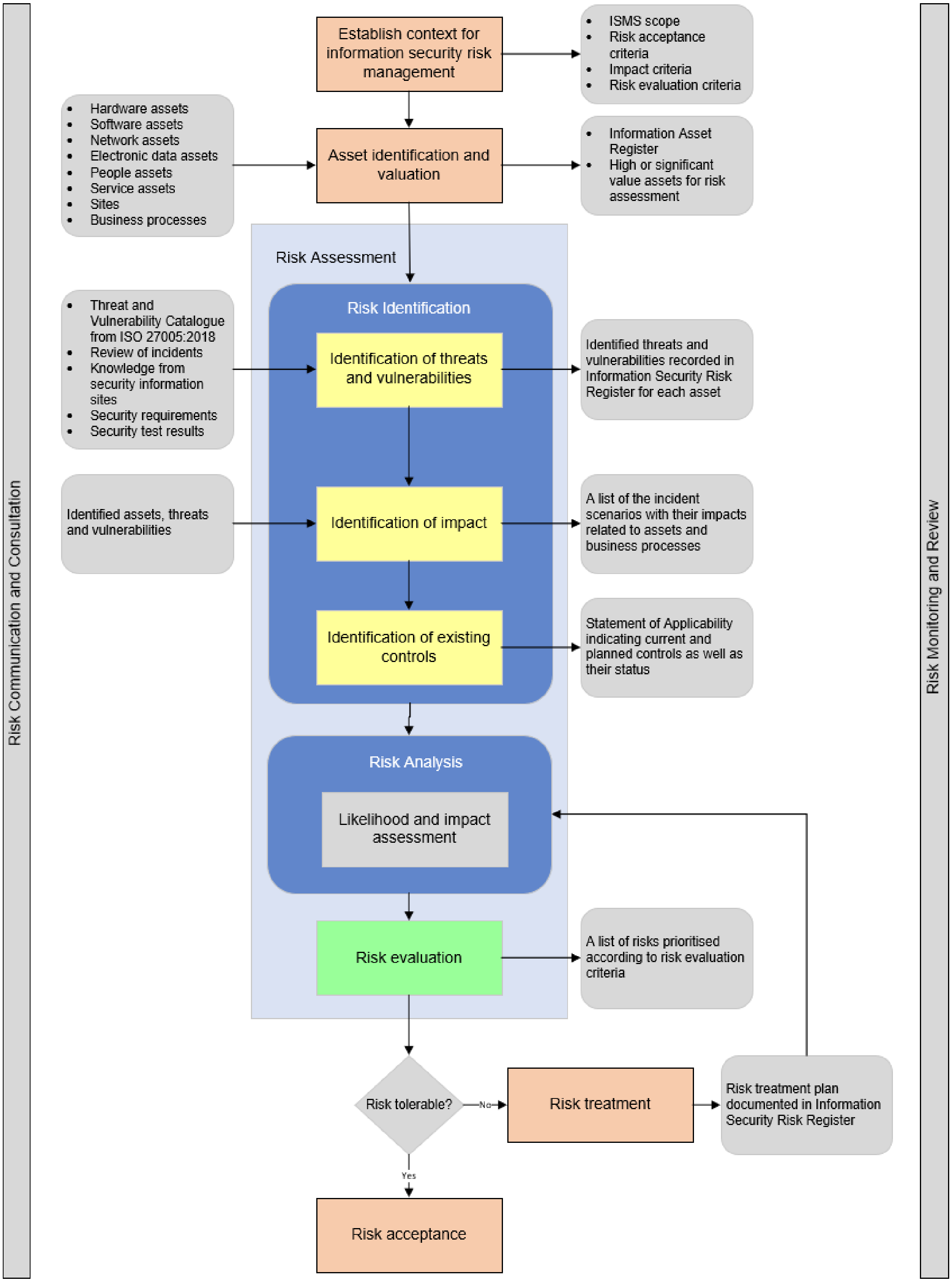

Risk Communication and Consultation
Risk Monitoring and Review
Establish context for information security risk management
ISMS scope
Risk acceptance criteria
Impact criteria
Risk evaluation criteria
Hardware assets
Software assets
Network assets
Electronic data assets
People assets
Service assets
Sites
Business processes
Asset identification and valuation
Information Asset Register
High or significant value assets for risk assessment
Risk Assessment
Risk Identification
Threat and Vulnerability Catalogue from ISO 27005:2018
Review of incidents
Knowledge from security information sites
Security requirements
Security test results
Identification of threats and vulnerabilities
Identified threats and vulnerabilities recorded in Information Security Risk Register for each asset
Identified assets, threats and vulnerabilities
Identification of impact
A list of the incident scenarios with their impacts related to assets and business processes
Identification of existing controls
Statement of Applicability indicating current and planned controls as well as their status
Risk Analysis
Likelihood and impact assessment
Risk evaluation
A list of risks prioritised according to risk evaluation criteria
Risk tolerable?
No
Risk treatment
Risk treatment plan documented in Information Security Risk Register
Yes
Risk acceptance

Figure 2: - Risk Assessment Steps

3.0 RISK ASSESSMENT CONTEXT

During the information risk assessment process, it is essential to establish the business context in which an information asset is to be assessed. Establishing the context ensures that the businesses objectives are captured and that the internal and external issues that influence the risks are considered. It also sets the scope for the rest of the process

3.1 BUSINESS CONTEXT

Meet with the Information asset owner to establish the business context. During the meeting, the asset owner is responsible for identifying and defining the:

- Information Classification – the information stored, processed and/or transmitted must be assigned an official classification based on the Data Classification Procedure (6000300).
- Business Processes Supported – the business processes and objectives supported by the information asset. This should include any secondary, dependent, or supporting processes.
- Users of the System – the different types of users of the information asset. This should include the level of privileges they require to perform their duties or to use the system. Users may include business users; operations support staff and external users of services such as members of the public or other third parties.
- C.I.A Value – the confidentiality, integrity, availability (CIA) requirements that is applied to the information asset, together with any relevant laws and/or regulations that need to be met.

4.0 INFORMATION ASSET IDENTIFICATION

Information Asset identification is the first step in risk assessment approach and plays a key role in the overall risk assessment process. The information assets within the established scope of STEPS' ISMS should be identified. Information asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment. All identified information assets should be recorded in an *Information Asset Register*. Information assets to consider are:

- Vital information for the functioning of STEPS' business processes
- Personal information, as defined by the *Privacy Act*
- Strategic information required for achieving STEPS' objectives
- High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

An asset owner should be identified for each asset, to provide responsibility and accountability for the asset. Information that is not identified as sensitive after this activity have no defined classification in the remainder of the risk assessment and risk treatment process.

5.0 ASSET VALUATION

Asset valuation is a major factor in risk assessment. In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business. Importance of an asset to the business is evaluated in terms of the impact of the loss of confidentiality (C), integrity (I) and availability (A) of the asset could have to the business.

5.1 ASSET VALUE

In order to consistently assess the asset values, and to relate them appropriately, a value scale for assets is applied. The loss of confidentiality (C), integrity (I) and availability (A) parameters for information assets are rated as follows:

- 1 – Low (L)
- 2 – Medium (M)
- 3 – High (H)

Table 1: - C*I*A Levels

The value of levels for Confidentiality, Integrity and Availability are taken as follows.

Levels	1 - Low	2 - Medium	3 - High
Confidentiality	Non-sensitive information available for public disclosure. The impact of unauthorised disclosure of such information shall not harm the organisation in anyway. Examples: • Press releases • Information on company website • Brochures	Information belonging to the organisation and not for disclosure to public or external parties. The unauthorised disclosure of information here can cause a limited harm to the organisation. Examples: • Internal policies and procedures	Information, which is very sensitive or private, of highest value to the organisation and intended to use by named individuals only. The unauthorised disclosure of such information can cause severe harm. Examples: • Board documents • Business plans • Client pricing information • HR records • Financial records
Integrity	There is minimal impact on the business if the accuracy and completeness of information is degraded.	There is significant impact on the business if the accuracy and completeness of information is degraded.	Result in critical impact to the business.
Availability	There is minimal impact on the business if the asset / information is unavailable.	There is significant impact on the business if the asset / information is unavailable.	Availability of the asset / information is critical to the business.

Asset value is computed as follows:

Asset Value = Confidentiality Level + Integrity Level + Availability Level

Table 2: - Asset Valuation Matrix

			Asset Valuation Matrix							
	Confidentiality	Low			Medium			High		
	Integrity	L	M	H	L	M	H	L	M	H
Availability	Low	3	4	5	4	5	6	5	6	7
	Medium	4	5	6	5	6	7	6	7	8
	High	5	6	7	6	7	8	7	8	9

Depending on the asset value, a qualitative level is assigned to the asset as per the following table:

Table 3: - Asset Value

	Value to the organisation	
Asset Value Level	**Asset Value (Numeric)** *Based on valuation matrix*	**Considered for Risk Assessment**
Significant	9	Yes (Top Priority)
High	7 - 8	Yes (High Priority)
Medium	5 - 6	Yes (Less Priority)
Low	3 - 4	No

6.0 RISK IDENTIFICATION

The first step of completing the *Information Security Risk Register* is to identify the risk stories that may impact the information security of the business. Stories are high level risk statements such as "There is a risk that an unauthorised party obtains access to private information". There may be numerous risk stories for a given organisation.

Secondly the business will identify the consequences for the organisation and impacted parties if that risk is realised. In the above example the consequences could be “Loss of contract, investigation by regulators, legal liability, identity theft, etc”.

Lastly you will identify the possible causes of that risk. There will likely be many causes for a given risk story. In the example above the causes could range through “External hacking of database, Incorrect access level given to employee, deliberate misuse or disclosure by employee, transmission snooping and interception, Information not stored correctly, etc”. You will notice the causes range in level of malicious intent and perpetrator, and thus will have different risk ratings and may have different controls associated with them.

6.1 IDENTIFICATION OF EXISTING CONTROLS

A control can reduce the risk by reducing the likelihood of an event, the impact or both. Existing controls in place must be identified.

Assessing the effect that the control has on the overall risk leads to determining the risk rating. The figure below can be used to identify the effect each type of control has on the likelihood or impact of a risk. Typically, deterrent, and preventive controls reduce the likelihood of a risk occurring whereas detective and corrective controls reduce the impact should the risk materialise.

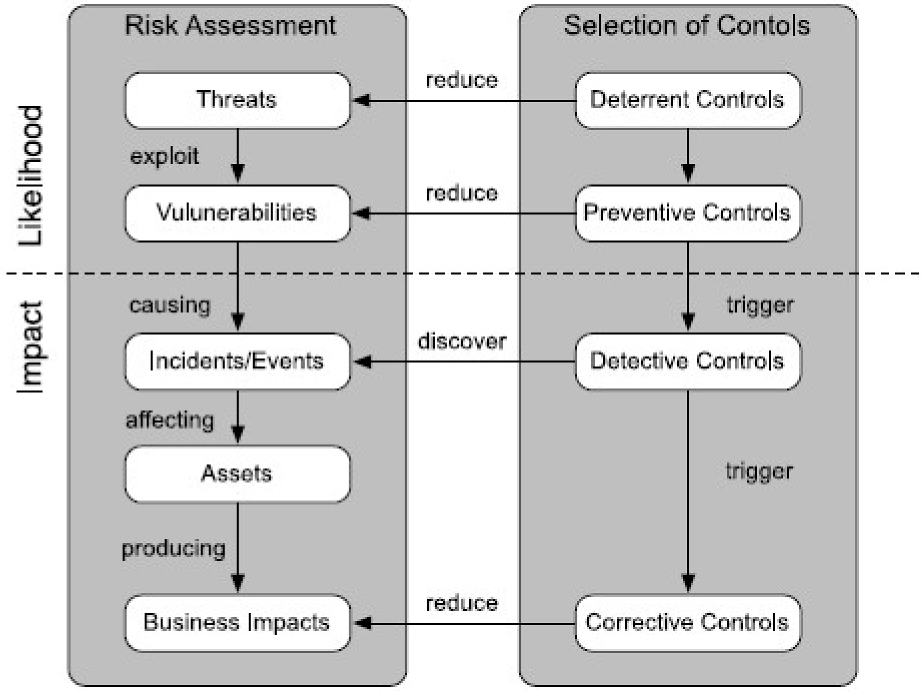


Figure 4: - Control Identification and Assessment

The following provides a brief description and some example for each type of control highlighted in Figure 4:

- **Deterrent Controls** – are intended to discourage a potential attacker. For example, establishing an information security policy, a warning message on the logon screen, a Kensington lock or security cameras.
- **Preventive Controls** – are intended to minimise the likelihood of an incident occurring. For example, a user account management process, restricting server room access to authorised

personnel, configuring appropriate rules on a firewall or implementing an access control list on a file share.

- **Detective Controls** – are intended to identify when an incident has occurred. For example, review of server or firewall security logs or Intrusion Detection System (IDS) alerts.
- **Corrective Controls** – are intended to fix information system components after an incident has occurred. For example, data backups, SQL transaction log shipping or business continuity and disaster recovery plans.

For the identification of existing or planned controls, the following activities will be conducted:

- Reviewing documents containing information about the controls (for example, risk treatment implementation plans). If the processes of information security management are well documented all existing or planned controls and the status of their implementation should be available.
- Checking with the people responsible for information security (e.g. information security officer, building manager or operations manager) and the users as to which controls are really implemented for the information process or information system under consideration.
- Conducting an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented as to whether they are working correctly and effectively, or reviewing results of previous audits.

7.0 RISK ANALYSIS

Once the relevant risks have been identified, the consequences understood, along with the causes and controls in place, then we can assess the risk rating of that risk being realised. The risk rating is composed of a combination of the likelihood of that risk being realised and the impact if the risk is realised.

7.1 IMPACT ANALYSIS

Impact scale is an estimate of the severity of adverse effects on business due to the risk.
Impact= Consequences due to a particular event.

Impact of the risk eventuating is analysed considering the existing controls in place.

Impact is considered as having either an immediate (operational) effect or a future (business) effect that includes loss of confidentiality, integrity and availability of the assets, financial and market consequences. Immediate (operational) impact is either direct or indirect.

Direct:

The financial replacement value of lost (part of) asset.

a) The cost of acquisition, configuration and installation of the new asset or back-up.

b) The cost of suspended operations due to the incident until the service provided by the asset(s) is restored.

c) Impact results in an information security breach (e.g. loss of confidentiality, integrity, and availability).

Indirect:

a) Opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere).

b) The cost of interrupted operations.

c) Potential misuse of information obtained through a security breach.

d) Violation of statutory or regulatory obligations.

e) Violation of ethical codes of conduct.

The table below presents a qualitative scale that should be used to describe the potential impacts.

Table 5: - Impact Scale

Level	Information Effect	Legal & Compliance	Service Disruption	Financial	Reputational
Extreme (5)	• Business disruptions resulting from malicious activity that results in > 50% service degradation • Any incident that impacts the availability of perimeter security infrastructure • Exposure of unencrypted, unmasked, or insufficiently masked confidential or sensitive information (inc. PII data) into the public domain or to an unauthorised third-party.	Major litigation costing $>50k; Investigation by regulatory body resulting in long term interruption of operations	An incident affecting any, or all of the STEPS Group of Companies	Event impact on income > $50k. Intense scrutiny from financial community (e.g. ATO).	Prolonged adverse national media attention or widespread condemnation. Loss of nationwide client.
High (4)	• Compromised privileged account credentials • Incident involving highly critical assets • >20% of the organisations users	Major breach of regulation with punitive fine, and significant litigation involving many weeks of senior management time with between $10k-$50k legal costs	An incident affecting multiple services, user groups, or network	Event impact on income before tax between $10k - $50k.	Major adverse national media attention. Loss of a state-wide client. Regulatory body investigation

Table 5: - Impact Scale

Level	Information Effect	Legal & Compliance	Service Disruption	Financial	Reputational
	unable to use ICT resources • Potential for involvement of law enforcement • Active attack incidents by unknown attackers that impact organisation's servers				
Moderate (3)	• Malware incidents that don't fall in a higher severity • Data loss incidents not involving sensitive information • Confirmed phishing campaign that impacts more than a dozen users	Breach of regulation with investigation by authority and possible moderate fine, and litigation and legal costs up to $9,999	An incident affecting one office, or group of users	Event impact on income before tax between $2.5k - $10k.	Significant adverse local media attention and/or heightened concern by local community. Impact on client's reputation / litigation from client.
Minor (2)	No loss of restricted, or business information that would not otherwise be publicly available. Minor impact on the integrity of information and minor impact on the availability of information.	Breach of regulations; major fine or legal costs; minor litigation	Some localised service disruption	Event impact on income between $500 - $2.5k.	Minimal adverse local media attention and/or heightened concern by local community. Complaints on client's reputation/ threat of litigation from client.

Table 5: - Impact Scale

Level	Information Effect	Legal & Compliance	Service Disruption	Financial	Reputational
Negligible (1)	No loss of restricted, or business information that would not otherwise be publicly available. No impact on the integrity of information and no impact on the availability of information.	Minor legal issues or breach of regulations	Minimal disruption	Event impact on income less than $500.	Complaint from local community that can be managed within 3 working days.

7.2 LIKELIHOOD (PROBABILITY)

Likelihood of the risk materialising is assessed considering the existing controls in place. Where information is available about the frequency of an incident in the past it should be used to determine the likelihood of the risk materialising. This information can be fetched from incident reviews, audit reports etc. However, where such information does not exist it does not necessarily mean that the likelihood of the risk materialising is low. It may merely indicate that there are no controls in place to detect it or that STEPS has not previously been exposed to the particular risk.

Table 6: - Likelihood Scale

Likelihood	Frequency	Qualitative	Quantitative Probability
Almost Certain (5)	10 times a year or greater	**Always** occurs within STEPS and/or the industry.	> 95%
Very Likely (4)	2 to10 times a year	**Periodically** occurs within company and/or the industry.	> 75% to 95%
Likely (3)	Once a year	**Occasionally** occurs within company and/or the industry.	> 30% to 75%
Unlikely (2)	Once every 2 to 9 years	**Infrequently** occurs within company and/or the industry.	5% to 30%
Very Unlikely (1)	Greater that every 10 years	**Has never occurred** in STEPS and/or the industry.	< 5%

Notes

- Frequency is based on evidence or data of risk occurring.
- Qualitative is used when no data is available to inform occurrence.
- Quantitative probability is used only on factored risk in projects – discrete values may be used.
- Likelihood is a rating that indicates the probability that a potential risk event will be realised, the current control environment must be considered when determining the likelihood.

8.0 RISK RATING

The risk rating is evaluated using the risk matrix presented in below table. It is used by mapping the likelihood and impact ratings for each risk.

Table 7: - Risk Matrix

Risk Matrix		Impact				
		Negligible (1)	Minor (2)	Moderate (3)	High (4)	Extreme (5)
Likelihood	Almost Certain (5)	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
	Very Likely (4)	MEDIUM	MEDIUM	HIGH	HIGH	EXTREME
	Likely (3)	LOW	MEDIUM	MEDIUM	HIGH	HIGH
	Unlikely (2)	LOW	LOW	MEDIUM	MEDIUM	HIGH
	Very Unlikely (1)	LOW	LOW	LOW	MEDIUM	MEDIUM

9.0 RISK RATING, SCALE AND TOLERANCE

Table 8: - Risk Rating and Risk Scale

Risk Level	Tolerance	Level of authority required to accept the risk	Indicative action required
Extreme	No tolerance	Managing Director and Board	1. Correction to be implemented with corrective action as part of a Risk Treatment Plan to be implemented within 3 months or the risk to be formally accepted by the risk owner and evidence recorded in the ***Information Security Risk Register***. 2. Reviewed at annual Management Review Meeting
High	Short term exposure less than 1 month	Executive Leadership Team	1.Correction to be implemented with corrective action as part of a Risk Treatment Plan be implemented within 9 months or the risk to be formally accepted by the risk owner and evidence recorded in the ***Information Security Risk Register***. 2. Reviewed at annual Management Review Meeting
Medium	Medium term exposure between 1 and 6 months	Executive Leadership Team Member	1.Correction to be implemented with corrective action as part of a Risk Treatment Plan to be implemented within 18 months or the risk to be formally accepted by the risk owner and evidence recorded in the ***Information Security Risk Register***. 2. Reviewed at ISMS Working Group Meetings.
Low	Long term exposure up to 12 months	Information Asset Owner	1. Monitored by normal business process as an acceptable risk. 2. Reviewed at ISMS Working Group Meetings.

10.0 RISK OWNER

Each risk must have a Risk Owner identified and appointed in the *Information Security Risk Register* with the appropriate authority and responsibility for managing the identified risk(s). The Chief Administrative Officer is responsible for working with the Risk Owner to formulate a risk treatment plan and obtain the Risk Owner's approval of the plan.

11.0 RISK EVALUATION

Once the risk analysis has been completed, the residual risks can be evaluated against the risk tolerance levels. Residual risks that are assessed as being low risk are generally considered to present an acceptable level of risk to the business and do not require any further evaluation. However, because risk is rarely static, a record of such risk should be maintained so that they can be monitored and assessed on a regular basis to ensure that the likelihood and/or impact do not change. Re-evaluation will be conducted when the risk treatment plan has been implemented or if there is a change in knowledge about the risk.

12.0 RISK TREATMENT

The risk treatment is the process of managing the risks by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable. Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options. *Information Security Risk Register* includes risk treatment plan which clearly identifies the timeframes in which individual risk treatments should be implemented.

Once the risk treatment plan has been defined, residual risks need to be determined. This involves an update or re-iteration of the risk assessment, taking into account the expected effects of the proposed risk treatment. Should the residual risk still not meet STEPS' risk acceptance criteria, a further iteration of risk treatment may be necessary before proceeding to risk acceptance.

12.1 RISK TREATMENT OPTIONS

There are four options available for risk treatment:

- **Risk Avoidance:** Risk can be avoided by stopping the activity that would give rise to the risk, thus eliminating the risk. Risk avoidance is not commonly selected as it typically results in not being able to exploit the associated opportunity.
- **Risk Modification / Reduction:** Risk can be modified or reduced by implementing, removing, or altering controls to reduce the likelihood and/or impact of the risk eventuating. This is the most commonly selected risk treatment.
- **Risk Retention / Acceptance:** Risk can be retained when the Risk Owner chooses to accept a risk. Risks are usually accepted when they are assessed as being within the business's defined risk tolerance level. However, they may also be accepted when it is not practical to avoid, treat or transfer the risk.
- **Risk Sharing:** Risk can be shared by transferring all or part of the impact of the risk eventuating with a third party. The most common risk transfer techniques are insurance and outsourcing.

13.0 FREQUENCY FOR CONDUCTING RISK ASSESSMENT

Risk assessment will be reviewed and updated

- At least on an annual basis for all information assets under the ISMS scope.
- When business environment and / or information systems change that could impact information security.

- When there is an information security incident

14.0 HOW TO RAISE A RISK

Employees or contractors can raise a risk by making direct contact with the Chief Administrative Officer or a member of the Executive Leadership Team.

15.0 HOW RISKS WILL BE MANAGED

The ISMS Working Group will:

1. Review the reported risk and confirm that the relevant information asset is listed in the *Information Asset Register*
2. Work with the assigned Risk Owner to complete the information security risk assessment to determine if the level of risk is acceptable or not:
    a. If acceptable:
        i. In the *Information Security Risk Register* complete the fields up to risk treatment option and select "Accept/retain"
    b. If not acceptable:
        i. In the *Information Security Risk Register* select one of the following risk treatment options:
            1. Risk avoidance
            2. Risk modification / reduction
            3. Risk sharing
        ii. Complete the risk treatment plan in consultation with the Risk Owner and then determine the residual level of risk
        iii. Set a deadline for the implementation of the risk treatment plan actions and change the status to open
3. Review the *Information Security Risk Register* at the ISMS Working Group meetings to update the status of the risk treatment plan and change the status of actions to closed when they have been addressed
4. On completion of the risk treatment plan, work with the Risk Owner to evaluate the effectiveness of the actions taken and determine if the treated risk is acceptable or requires re-evaluation and further risk treatment.

16.0 RELATED DOCUMENTS

Document Name	Document Name
Data Classification Procedure (6000300).	*The following ISMS Registers are located under* ISMS-Registers • *Information Asset Register* • *Information Security Risk Register*

ISMS Manual (6000004)	ISMS Scope *(6000005)*

17.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	23 June 2022
Effective Date	24 June 2022	**Document Number**	6001300_v2_220624

(Uncontrolled when printed)

1.9.2.15 Third Party Connection Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as "STEPS."

1.1 DEFINITIONS

Access Control List (ACL)	A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.
Demilitarized Zone (DMZ)	A perimeter network, typically inside the firewall but external to the private or protected network, where publicly accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.
Firewall	A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.
Third Party Connection	A direct connection to a party external to STEPS. Examples of third-party connections include connections to customers, vendors, partners, or suppliers.

2.0 PROCEDURE

2.1 USE OF THIRD PARTY CONNECTIONS

Third party connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third-party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the Technology & Cyber Security Manager.

2.2 SECURITY OF THIRD PARTY ACCESS

Third party connections require additional scrutiny. The following statements will govern these connections:

- Connections to third parties must use a firewall or Access Control List (ACL) to separate STEPS' network from the third party's network.
- Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible, this should include time-of-day restrictions to limit access to only the hours when such access is required.
- Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) to protect internal network resources.
- If a third-party connection is deemed to be a serious security risk, the Technology & Cyber Security Manager will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be implemented at the recommendation of the Technology & Cyber Security Manager.

2.3 RESTRICTING THIRD PARTY ACCESS

Best practices for a third-party connection require that the link be held to higher security standards than an intra-company connection. As such, the third party must agree to:

- Restrict access to STEPS' network to only those users that have a legitimate business need for access.
- Provide STEPS with the names and any other requested information about individuals that will have access to the connection. STEPS reserves the right to approve or deny this access based on its risk assessment of the connection.
- Supply STEPS with on-hours and off-hours contact information for the person or persons responsible for the connection.
- (If confidential data is involved) Provide STEPS with the names and any other requested information about individuals that will have access to STEPS' confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

2.4 AUDITING OF CONNECTIONS

To ensure that third-party connections are compliant with this procedure, they must be audited quarterly.

2.5 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the ICT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name
Nil

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6001400_v2_230601

(Uncontrolled when printed)

1.9.2.16 VPN Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 DEFINITIONS

Certificate	Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.
Demilitarized Zone (DMZ)	A perimeter network, typically inside the firewall but external to the private or protected network, where publicly accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.
Encryption	The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
Remote Access VPN	A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.

Site-To-Site VPN	A VPN implemented between two static sites, often different locations of a business.
Virtual Private Network (VPN)	A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

2.0 PROCEDURE

2.1 ENCRYPTION

Site-to-site VPNs must utilise strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as Triple DES or AES.

2.2 AUTHENTICATION

Site-to-site VPNs must utilise a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

2.3 IMPLEMENTATION

When site-to-site VPNs are implemented, they must adhere to the procedure of least access, providing access limited to only what is required for business purposes. This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes.

2.4 MANAGEMENT

STEPS manages its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the Technology & Cyber Security Manager.

2.5 LOGGING AND MONITORING

Depending on the nature of the site-to-site VPN, the Technology & Cyber Security Manager will use his or her discretion as to whether additional logging and monitoring is warranted. As an example, a site-to-site VPN to a third party would likely require additional scrutiny but a VPN to a site office of STEPS would likely not be subject to additional logging or monitoring.

2.6 ENCRYPTION KEYS

Site-to-site VPNs are created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Encryption keys should be changed periodically.

If certificates are used instead of pre-shared keys, the certificates should expire and be re-generated after three years.

2.7 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name
Nil

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6001500_v2_230601

(Uncontrolled when printed)

1.9.2.17 Wireless Access Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as “STEPS.”

1.1 DEFINITIONS

Mac Address	Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.
SSID	Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

WEP	Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.
WiFi	Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.
Wireless Access Point	A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.
Wireless NIC	A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.
WPA	Stands for Wi-Fi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

2.0 PROCEDURE

2.1 PHYSICAL GUIDELINES

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points should be located central to the office space rather than along exterior walls. Technology should be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas must be used as necessary to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must be placed in secured areas of the office. Cabling to and from access points should be secured so that it cannot be accessed without difficulty.

2.2 CONFIGURATION AND INSTALLATION

The following guidelines apply to the configuration and installation of wireless networks:

2.2.1 Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default.
- The Service Set Identifier (SSID) for non-public use must not use company naming.
- Administrative access to wireless access points should utilise strong passwords.
- Encryption should be used to secure wireless communications. Stronger algorithms are preferred to weaker ones (i.e., WPA should be implemented rather than WEP).

2.2.2 Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) should be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent STEPS' security controls.
- Wireless devices should be installed only by STEPS' ICT department.
- Channels used by wireless devices should be evaluated to ensure that they do not interfere with company equipment.

2.3 ACCESSING CONFIDENTIAL INFORMATION

Wireless access to confidential data is permitted if the access is consistent with this and other policies that apply to confidential data.

2.4 INACTIVITY

Users should disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC.

Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to STEPS.

2.5 AUDITS

The wireless network will be periodically audited by the Cyber Security & Systems Engineer to ensure that this procedure is being followed. Specific audit points should be location of access points, signal strength, SSID, and use of strong encryption.

2.6 APPLICABILITY OF OTHER PROCEDURES

This document is part of STEPS' cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

3.0 ENFORCEMENT

This procedure will be enforced by the Technology & Cyber Security Manager and/or Executive Leadership Team (ELT). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe consequences up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, STEPS may report such activities to the appropriate authorities.

4.0 RELATED DOCUMENTS

Document Name
Nil

5.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	1 June 2023	**Document Number**	6001600_v2_230601

(Uncontrolled when printed)

1.9.3 System Security Plans

BuddyNote

1.10 Privacy and Data Breach

Enter topic text here.

1.10.1 Complying with the Australian Privacy Principles

1.0 INTRODUCTION / GENERAL

STEPS are obligated by the Commonwealth Privacy Laws which regulate the collection and handling of personal information through minimum privacy standards, known as the.Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) Act. The APPs apply to STEPS and they must be complied with in all services provided by STEPS. For specific information about APPs, see the reference document APP – A summary for APP Entities.

Where STEPS provides services on behalf of government departments, they are required to use the Privacy Notice provided which details how an individual's personal information will be handled. These notices need to be explained to customers, participants, and students at the commencement of services with STEPS and it is a requirement of the contract that the privacy notice is complied with.

This procedure outlines how STEPS Group of Companies (STEPS) expects employees and volunteers to handle personal information collected and held by STEPS.

1.1 DEFINITIONS

APP	Australian Privacy Principles

2.0 PRIVACY DEFINED

What is Privacy?

- Privacy is the right to be able to control who can see or use information about an individual.

Whose Privacy does STEPS protect?

- STEPS respects and protects the privacy of its customers, participants, and students.

How do STEPS protect Privacy?

STEPS have developed organisational policies, procedures, and processes which all employees and volunteers must adhere to protect customer, participants, and student stored information, such as:

- not sharing passwords
- not leaving hardcopy files in view
- locking computer screens when away from desk
- carefully checking email addresses to ensure the correct recipient etc.

Who is responsible for protecting privacy?

Each Site Manager has overall accountability for privacy in the site they manage. STEPS employees and volunteers:

- have a role to play in ensuring the privacy of customers, participants and students is respected and protected.
- must ensure that personal information is stored / retained for periods of time as contained in legislation and in the relevant contracts or grants.
- are required to discuss any issues or concerns with privacy processes and procedures with their line manager, a member of the Quality Assurance & Risk Team or the STEPS Privacy Officer at cso@stepsgroup.com.au .

STEPS Privacy Officer is often the first point of contact, responding to enquiries and may coordinate access and correction requests and complaints about STEPS' personal information handling practices.

The Quality Assurance & Risk Team understands STEPS' responsibilities under the Privacy Act and contracts and will undertake the development of policy and procedures.

3.0 PERSONAL INFORMATION

In most circumstances employees and volunteers will only have access to personal information that they need for their role or function. By limiting the personal information employees and volunteers have access to, STEPS is helping to protect personal information from unauthorised access, use or disclosure. The APPs provide higher privacy standards when organisations are handling an individual's sensitive information.

What is Personal Information?

- Personal information is information that identifies a person.

Through its various services and to conduct its day-to-day business, STEPS collect a range of personal information where the person is reasonably identifiable which may include:

- a person's name or address
- photos
- bank account details
- credit history information
- where they work
- information about what a person likes and their opinions

Personal information can be sensitive in nature including:

- a person's race, ethnicity, political opinions
- religious or philosophical beliefs
- sexual preferences
- membership of political associations
- professional associations and trade unions

- health and genetic information or criminal records

Personal information should be stored / retained for periods of time as contained in legislation and in the relevant contracts or grants.

3.1 COLLECTING PERSONAL INFORMATION

All services provided by STEPS adhere to the following principles when collecting personal information:

- Collect information lawfully and fairly.
- Collect information and any consent needed directly from the individual unless it is unreasonable or impractical to do so.
- Provide notice to individuals about the potential collection, use and disclosure of personal information.
- Limit the collection of information to that which is needed for the purpose it is being collected.
- Only collect personal information that is needed at the time. Do not collect personal information just because it may become necessary or useful later. If it is needed later, the information can be collected then.
- All customers, participants and students should know what personal information is collected and why.
- When describing the information being collected take special care to explain if sensitive information will be collected.
- In most cases personal information is collected directly from the individual, usually by completing forms or through interviews.
- Other information can be collected indirectly and where this occurs the individual will usually be required to give permission for that information to be obtained.
- When information is no longer needed it should be stored securely, de-identified or destroyed.

3.2 USING PERSONAL INFORMATION

All employees and volunteers of STEPS are to only use or disclose personal information for the primary purpose for which it was collected. Prior to using or disclosing personal information, employees and volunteers should give consideration to:

- whether the service, support or business activity can be conducted without using or disclosing personal information
- the amount of personal information used or disclosed should be kept to the minimum necessary

There are exceptions that allow the use or disclosure of personal information for another purpose, which include where:

- the individual has consented to the use or disclosure
- the individual would reasonably expect the use or disclosure and the other purpose relates (or for sensitive information, directly relates) to the primary purpose of collection
- the use or disclosure is required or authorised by law

3.3 STORING PERSONAL INFORMATION

STEPS, as an organisation and all employees and volunteers must adhere to measures put in place to protect stored information, such as:

- not sharing passwords
- not leaving hardcopy files in view
- locking computer screens when away from desk
- carefully checking email addresses to ensure the correct recipient etc.
- not including multiple recipient email addresses in the ‘TO’ or ‘CC’ section of an email

- only using ‘blind copy’ when sending multiple recipient email addresses in one email.

Storage of personal information occurs if:

- personal information is stored in a third-party storage provider (such as MYP, Wisenet)
- there is a link to other personal information held about an individual (ESS web, Unique Student Identifier)

Personal information should be stored / retained for periods of time as contained in legislation and in the relevant contracts or grants.

3.4 DISCLOSING OF PERSONAL INFORMATION

Where an individual’s personal information is going to be shared with any other organisation or government department STEPS employees and volunteers must explain this to the individual. The disclosure of personal information is usually most important to individuals. Information disclosures are often contained in Privacy Notices which must be provided to individuals at the commencement of any service.

It is important to note that if a third party mishandles data held on behalf of STEPS, it is very likely that STEPS will bear the commercial and reputational damage.

3.5 POTENTIAL THREATS TO PERSONAL INFORMATION

STEPS, and all STEPS employees and volunteers must take reasonable steps to protect personal information from unauthorised access, modification, or disclosure and against misuse, interference, and loss.

If an employee or volunteer becomes aware of personal information being accessed, modified or disclosed (or the potential for this to occur; for example a stolen laptop) without the individual’s consent, or one of STEPS software systems has been compromised they should inform their Manager and complete the Data Breach Report (i020501).

The Data Breach Report (i020501) assists STEPS in responding quickly and appropriately in the case of a data breach. A quick response may stop a potential breach, or substantially decrease the impact on the affected individuals. If there is a data breach and there is risk of serious harm to the affected individuals, STEPS may be required to notify the Office of the Australian Information Commissioner (OAIC).

To prevent a data breach Managers are required to ensure that all employees and volunteers are familiar with and follow:

- STEPS’ policies and procedures on information security, including ICT security (such as password management)
- physical security
- access security
- always destroy and de-identify personal information in accordance with record keeping procedures

Human error is a large source of security breaches, so all employees and volunteers need to be familiar with the APPs and always act in a way that upholds the principles and complies with this procedure.

4.0 INDIVIDUALS RIGHTS AND CHOICES

The Privacy Act requires that all personal information kept is accurate, complete, and up to date. For this reason, file notes or progress notes need to be recorded in the appropriate format as soon as practicable. Managers should ensure that accurate information is always held by regularly checking the accuracy of information held (i.e., change to address or phone number).

Individuals have the right to:

- request access to information held about them, please refer to the Request to Access Personal Information (i020600)
- request correction of personal information held about them

If the person requests a correction that is in dispute (i.e., STEPS has a different view of what occurred) the individual's perspective should be recorded as per their request, noting that there are differences in the records held. STEPS can decide not to make changes to the file notes made by a STEPS employee or volunteer.

5.0 HOW TO MAKE A COMPLAINT

If an individual is not happy with the way their personal information is handled by STEPS they should use the complaints process as stated in the Feedback Procedure (i040100) and Complaints Procedure (i040500).

If a customer, participant, or student is not satisfied with the outcome they can complain to an external body. These are listed in the Feedback Procedure (i040100) and Complaints Procedure (i040500).

6.0 RELATED DOCUMENTS

Document Name	Document Name
Request to Access Personal Information (i020600)	Data Breach Report (i020501)
Feedback Procedure (i040100)	Complaints Procedure (i040500)

7.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	27 July 2023
Effective Date	8 August 2023	**Document Number**	i020700_v3_230808

(Uncontrolled when printed)

1.10.2 Data Breach Identification and Reporting

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is hereinafter referred to as "STEPS" must take reasonable action to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure in accordance with the Privacy Act 1988 (Privacy Act).

Part III C of the Privacy Act established requirements for entities responding to data breaches. Entities have data breach notification obligations (known as Notifiable Data Breach (NDB) scheme) when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

The NDB scheme sets out mandatory notification and control requirements for data breaches involving personal information held by an organisation. It outlines criteria for determining if a data breach is considered ‘eligible’ (notifiable) and the subsequent reporting requirements.

1.1 DEFINITIONS

Australian Privacy Principle (APP) Entity	An APP (Australian Privacy Principle) entity’ is defined in the Privacy Act to be an agency or organisation. An ‘organisation’ is defined to be: • an individual (including a sole trader) • a body corporate • a partnership • any other unincorporated association, or • a trust unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State.
Eligible Data Breach	Occurs when the following criteria are met: • There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised assess or disclosure is likely to occur). • This is likely to result in serious harm to any of individuals to whom the information relates. • The entity has been unable to prevent the likely risk of serious harm with remedial action.
Interference	Occurs where there is an attack on personal information that an APP entity holds that interferes with the personal information but does not necessarily modify its content. ‘Interference’ includes an attack on a computer system that, for example, leads to exposure of personal information
Loss	Applies to the accidental or inadvertent loss of personal information held by an APP entity. This includes: • physical losses (including hard copy documents, computer equipment or portable storage devices containing personal information), for example, by leaving it in a public place, or

	• electronic losses such as failing to keep adequate backups of personal information in the event of a systems failure. Loss may also occur as a result of theft following unauthorised access or modification of personal information or as a result of natural disasters such as floods, fires or power outages.
Unauthorised Access	Occurs when personal information that an APP entity holds is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity or independent contractor, as well as unauthorised access by an external third party (such as by hacking).
Unauthorised Modification	Occurs when personal information that an APP entity holds is altered by someone who is not permitted to do so or is altered in a way that is not permitted under the Privacy Act. For example, modification by an unauthorised employee, or following unauthorised access to databases by an external third party.
Unauthorised Disclosure	Occurs when an APP entity: • makes personal information accessible or visible to others outside the entity, and • releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the APP entity.
Data Breach Team (DBT)	Consists of the Managing Director, Chief Executive Officer, Chief Operating Officer, Chief Administrative Officer, Executive Manager HR and the Technology & Cyber Security Manager.
Serious Harm	This could include serious physical, psychological, emotional, economic and financial harm; and serious harm to reputation, distress or being upset would not itself be sufficient. Serious harm will be “likely” if it more probable than not, rather than possible.

2. IDENTIFYING A DATA BREACH

All employees are responsible for being aware of their obligations under the Privacy Act. Obligations can be found in the STEPS Privacy Policy (i010106), in particular Part A which refers to the Personal Information Handling Practices.

As soon as an employee becomes aware that there has been:

- Unauthorised access,
- Unauthorised disclosure, or
- Loss (hard copy and electronic, or portable devices)

of personal information they must notify their manager/supervisor immediately.

The manager/supervisor is responsible for ensuring that the identified data breach is recorded on the Data Breach Report (i020501) form which must be emailed to the Executive Manager within their line management and to the Privacy Officer/Customer Services Officer at cso@stepsgroup.com.au. If the Executive Manager is not available escalate to the Chief Executive Officer (CEO).

Please note that a data breach may not qualify as a Notifiable Data Breach, but it must be reported in order for the determination to the made by the Data Breach Team.

3. REMEDIAL ACTION

Remedial action can be taken, or requested at any time as soon as a possible data breach is identified (e.g. report lost mobile device to ICT; contact incorrect email recipient and ask them to permanently delete an email sent in error).

By taking remedial action STEPS has the opportunity to take positive steps to address a data breach in a timely manner. If this remedial action means that the data breach would not be likely to result in serious harm, then the breach is not an ‘eligible’ data breach, which means notifying the Commissioner and individuals would not be necessary.

Remedial action will be adequate if it prevents unauthorised access to, or disclosure of personal information. For example, if a mobile device (such as a phone or laptop) is lost and the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, this would mean that here is no eligible data breach.

4. REPORTING THE DATA BREACH

The Executive Manager will advise all members of the Data Breach Team; which includes the Managing Director, Chief Executive Officer, Chief Operating Officer, Chief Administrative Officer, Executive Manager HR, and the Technology & Cyber Security Manager.

4.1 If a data breach has been reported from within a program, refer to the Program Contracts – Data Breach Reporting Information form which outlines the action to be undertaken.

5. ASSESSING THE DATA BREACH

The Data Breach Team will gather relevant information and assess the data breach to determine if it is an eligible data breach using the Data Breach Assessment (i020502).

All parties will be required to provide information to the DBT in accordance with requested timeframes.

All reasonable steps to complete the assessment within five (5) business days after the day the entity became aware of possible data breach.

The CAO will provide finial approval of the assessment by applying an electronic signature.

6. EVALUATING THE DATA BREACH

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information held by STEPS
2. this is likely to result in serious harm to one or more individuals, and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

If the assessment determines that the data breach is an eligible data breach, an appropriate response will need to be implemented by the Data Breach Team.

7. NOTIFIABLE DATA BREACHES

Where the DBT determines that the 3 criteria are satisfied and an 'eligible' data breach has occurred STEPS must comply with the NDB scheme.

7.1 PREPARE DATA BREACH STATEMENT

STEPS must prepare a data breach statement as soon as practicable after becoming aware. This statement must contain:

- the entity's details
- a description of the breach
- the kinds for information concerned (using category e.g. "health information", "Driver's Licence number")
- recommendations about steps that affected individuals should take in response to the breach
- legal advice should be sought before including an apology in a statement.

Where a breach relates to jointly-held information the entities concerned may prepare a joint-statement. The Commissioner has determined this is not necessary where the individuals concerned do not have a relationship with the other entity.

7.2 NOTIFY COMMISSIONER

A copy of the Data Breach Statement must be provided to the Commissioner as soon as practicable after the entity becomes aware of the breach. This can be done through the Office of the Information Commissioner (OAIC) using an on-line form or by contacting them to make other arrangements.

There is no requirement to notify the Commissioner prior to notifying individuals. An entity can opt to notify individuals before notifying the Commissioner, this may be appropriate where there is a high level of urgency and it is preferable to focus resources on notifying individuals as soon as possible.

7.3 NOTIFY INDIVIDUALS

The statement must be provided to individuals concerned. There are three methods by which notification may be provided depending on the circumstances:

(a) Notify all individuals concerned – if it is practicable to notify each individual whose personal information was part of the breach, the entity must take reasonable steps to do so;

(b) Notify individuals at risk of serious harm - if it is practicable to notify each individual who is at risk of serious harm from the breach, the entity must take reasonable steps to do so;

(c) Publicise data breach statement – if direct notification is not practicable (e.g. where the entity does not have up-to-date contact details) the entity must publish the statement on its website and take reasonable steps to publicise the statement (e.g. social media post or advertisements in print or online media).

If providing notice to individuals STEPS' will need to consider if it can under the circumstances of each affected individual to determine which individuals are at risk and those who are not, where it may be more practical to notify an entire cohort.

If it can be determined with a high degree of confidence that only some individuals from a broader group are at risk, notifying the broader group may not be necessary to mitigate harm.

It is permitted to consider the time, effort and cost of notifying individuals at risk of serious harm in a particular manner.

8. COMMISSIONER'S RESPONSE

Once the Commissioner has received a data breach notification statement, his or her response will depend on the nature and scale of the breach and the responsive measures taken by the entity.

9. REVIEW THE INCIDENT

The incident should be reviewed to ensure that all steps are taken to reduce the likelihood of future breaches.

10. RELATED DOCUMENTS

Document Name	Document Name
Data Breach Report (i020501)	Data Breach Assessment (i020502)
Privacy Policy (i010106)	Programs – Contractual Data Breach Reporting Information (i020503)

10. GOVERNANCE

Document Owner	Chief Executive Officer	**Approval Date**	18 December 2023
Effective Date	15 January 2024	**Document Number**	i020500_v3_240115

(Uncontrolled when printed)

1.10.3 Request to Access to Personal Information

1.0 GENERAL

The *Privacy Act 1988* (Cth) was introduced to promote and protect the privacy of individuals and contains a list on minimum privacy standards known as the Australian Privacy Principles (APPs).

APP 12 requires an APP entity that holds personal information about an individual to give an individual access to that information on request.

APP 11.2 states that an APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure.

This means that STEPS' customers, participants, and students may request access to personal information held by STEPS and on request, STEPS must give the individual access to the information, unless there are grounds to refuse access, grounds for refusal are limited. Please note that the requirement for an entity to provide access to personal information, there is no right to access other kinds of information.

STEPS deliver a range of courses or programs which may have specific contractual requirements related to privacy, please refer to the SQM or the relevant Manager for clarification.

1.1 DEFINITIONS

Holds	Where the entity has possession or control of a records that contains personal information. The term 'holds' extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, where storage of personal information is outsources to a third party, but the entity retains the right to deal with that information, including to access and amend it, the entity must comply give the individual access (unless an exception applies). The individual cannot simply be referred to the third party that has physical possession. Records in the entities control may include hard coy records and electronic databases.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: • whether the information or opinion is true or not, and • whether the information or opinion is recorded in a material form or not'
Records that hold personal information of another individual	APP 12 requires an APP entity to provide access to all of an individual's personal information it holds, even if that information is also the personal information of another individual, unless a ground to refuse access applies. For example, information in a marriage certificate may be personal information of both parties to the marriage, and an opinion may be personal information of both the subject and the giver of the opinion.

2.0 ACCESS TO PERSONAL INFORMATION

When a request to access personal information is received by STEPS the employee receiving the request will: -

- complete the Request for Personal Information Form (i020601)
- inform the individual that STEPS Privacy Officer will contact them
- email the Request for Personal Information Form (i020601) to STEPS Privacy Officer at cso@stepsgroup.com.au.

STEPS Privacy Officer will: -

- contact the individual and request (where possible) they attend a face to face meeting at their closest STEPS site and bring in photo ID from the approved list which confirms their identification and signature. if the individual is unable to attend a face to face meeting the STEPS Privacy Officer is required to send the individual the Verification of Identity Form (i020602) and request that they provide one of the approved forms of ID listed on the form.
- create an individual folder in the 'O' Drive / Quality Processes / Release of Information Folder under the program under which the service was requested using their SURNAME-First Name as the naming convention.

2.1 VERIFYING AN INDIVIDUAL'S IDENTITY

STEPS must be satisfied that a request for personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent.

Proof of and verification of identity including the matching of the individual's signature against the signature held by STEPS is required prior to access or release of personal information.

Requests for access to personal information received from an authorised agent must include a request and approval from the individual for access or release of their personal information to the authorised agent. Verification of identity and signature matching must be completed.

If the individual is already known to or readily identifiable by STEPS (e.g. currently accessing a service) the employee receiving the request is required to complete the Request for Personal Information Form (i020601) and Verification of Identity Form (i020602) and forward this to the STEPS Privacy Officer at cso@stepsgroup.com.au.

Where possible the proof of identity should be sighted rather than copied or collected, for this purpose individuals requesting access to personal information should be encouraged to come into their closest STEPS site. In a face-to-face dealing with the individual, the STEPS employee should record which type of identity document (such as a Driver's Licence) was sighted, the number and confirm that the signature matches the one held on record by STEPS.

Where the individual requesting access to personal information is unable to come into the STEPS site, they are required to complete the Verification of Identity Form (i020602) and provide a form of photo ID on the approved list. The individual's signature can then be matched against the one held on record by STEPS.

2.2 RESPONSE TIMES

STEPS must respond to a request for access within 30 calendar days.

The response will either:

- provide the access to the personal information, or
- notify refusal to give access (refusal must be approved by the Managing Director (MD) or Chief Executive Officer (CEO).

If there are reasons why this time frame cannot be met (e.g. clarification is required, location of the information) then STEPS must contact the individual, explain the reason for the delay and provide an expected timeframe for finalising the request.

2.3 HOW ACCESS SHOULD TO BE GIVEN

Wherever possible STEPS should provide the information to the individual in the manner requested for example, by email, by phone, in person, hard copy, or an electronic record.

It may not be possible to give access in the manner requested. For example, it may be impracticable to provide a large amount of personal information by telephone.

If an individual has special needs it may be reasonable to give the information in a form that can be accessed via assistive technology to meet the special needs of the individual.

2.4 ACCESS CHARGES

STEPS cannot impose a charge on an individual for making a request to access personal information.

In exceptional circumstances STEPS may, however, impose a charge for giving access to requested personal information, provided the charge is not excessive. Any charge must be approved by the MD or CEO. Charges may include:

- staff costs in searching for, locating, and retrieving the requested personal information, and deciding which personal information to provide to the individual, or
- costs of postage or materials.

Wherever possible STEPS will waive, reduce, or share any charge imposed, to ensure any charge is not excessive.

3.0 REFUSING TO GIVE ACCESS

There are ten grounds on which STEPS can refuse to give access to personal information. The decision to rely on one of these grounds will need the approval of the MD or CEO. The individual making the request for personal information will need to be advised in writing of the decision.

3.1 GROUNDS FOR REFUSAL

The grounds for refusal are summarised below:

- STEPS believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety
- giving access would have an unreasonable impact on the privacy of other individuals (in this circumstance it is recommended that some information is redacted so that access can be provided)
- the request for access is frivolous or vexatious (e.g. a repeated requests for information that has been provided already)
- the information relates to existing or anticipated legal proceedings between STEPS and the individual, and would not be accessible by the process of discovery in those proceedings
- giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations

- giving access would be unlawful
- denying access is required or authorised by or under an Australian law or a court/tribunal order
- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body
- giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process

4.0 RECORD KEEPING

All requests to access personal information must be recorded on the Request for Personal Information Form (i020601). Verification of Identity must be recorded on the Verification of Identity Form (i020602) and where hard copy evidence is provided saved in the individual's folder located in the 'O' Drive / Quality Processes / Release of Information Folder.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Request for Personal Information Form (i020601)	Verification of Identity Form (i020602)

6.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	23 February 2021
Effective Date	18 March 2021	**Document Number**	i020600_v2_210318

(Uncontrolled when printed)

1.11 Quality Systems and Continual Improvement

Enter topic text here.

1.11.1 Audits

1.0 INTRODUCTION

As a quality assured organisation, STEPS Group of Companies (STEPS) conduct audits to ensure the Quality Management System (QMS) is effectively implemented and maintained. In addition, the services provided by STEPS may be certified against legislative standards (e.g. The National Standards for Disability Services, NDIS Practice Standards and Quality Indicators and National Standards for Mental Health Services).

To support internal audits, reviews and self-assessments can be undertaken where standards determine these are adequate and sufficient to demonstrate the ability of processes and procedures to achieve planned results and identify areas for improvement.

For the purpose of this procedure, financial audits do not apply. Further information about financial audits can be found in Financial Management (e310200).

The Quality Assurance and Risk team is responsible for coordinating the auditing processes.

Wherever possible, internal audits will be conducted by personnel independent of the operating processes being audited.

2.0 ACCESS TO EMPLOYEE FILES

During internal and/or external audits, auditors may require access to employee files to ascertain STEPS' performance against criteria relating to various human resource management activities including recruitment and selection, induction and learning and development activities.

STEPS Human Resources team members will manage and facilitate the viewing of all employee files in accordance with ISO 27001:2022 by sitting with the auditor and sharing their screen.

3.0 MASTER AUDIT SCHEDULE

The Risk and Compliance Manager is responsible for the development of the Master Audit Schedule (MAS) (i060101) with review by the Chief Administrative Officer (CAO).

In developing the Master Audit Schedule (MAS) (i060101), the following is considered:

- scheduled external Mid-Term Assessments
- scheduled external Recertification Audits
- audit requirements under specific standards or legislation
- specific audit evidence requirements of funding agreements/contracts e.g., Skills Assure Supplier (SAS) Agreement
- areas of the business which are at risk of non-compliance

The CAO will table the upcoming Financial Year's proposed Master Audit Schedule (MAS) (i060101) at the Executive Leadership Team (ELT) meeting for approval in May of each year.

The ELT will consider previous audit findings and risks in order to approve the Master Audit Schedule (MAS) (i060101). The CAO will notify the Risk and Compliance Manager of the outcome. When approved the Quality Assurance & Document Control Coordinator will upload the Master Audit Schedule (MAS) (i060101) to the relevant management operating system and maintain the schedule throughout the year.

4.0 TYPES OF AUDITS

4.1 INTERNAL AUDITS

STEPS conducts periodic internal audits, reviews, and self-assessments to identify areas for continual improvement. These are conducted by STEPS Managers and relevant staff and the Quality Assurance and Risk team under the guidance of the Risk and Compliance Manager.

4.2 OUTSOURCED INTERNAL AUDITS

STEPS engage a range of specialist external auditors to conduct outsourced internal audits across various programs/departments of the organisation. These internal audits are conducted in accordance with the Master Audit Schedule (MAS) (i060101) either onsite or remotely.

4.3 CERTIFICATION AUDITS

Certification, Mid-Term or Surveillance Assessments and Recertification Audits are conducted by accredited auditors approved by STEPS. The auditors will provide a detailed list of requirements, audit plan/assessment schedule and a dedicated portal for the upload of all documentation.

Prior to the audit, the accredited auditor will provide a Service Description of the audit which outlines key areas of the audit. The Quality Assurance & Document Control Coordinator will review the proposed activities and timing with reference to the MAS and in consultation with the appropriate department/program Manager, with approval to proceed to be provided by the CAO. Upon receipt of the auditor's Service Description the Quality Assurance & Document Control Coordinator will schedule a meeting with all impacted internal stakeholders. The objective of this meeting is to ensure all stakeholders know what is required of them and their teams to enable effective and efficient management of the audit. The Quality and Risk Manager will communicate the audit objectives, scope, approach and timing. During this meeting responsibilities and timelines for the submission of files requested by the auditor and any other supporting evidence will be agreed.

A confirmation meeting will be held the week prior to the audit to ensure all stakeholders are prepared.

Certification audits are divided into two stages – **Stage 1** which is a desktop audit of policies and procedures. **Stage 2** which may be conducted onsite or remote, includes a review of policies, procedures and meetings with staff and participants.

When notified of external audits, the Quality Assurance & Document Control Coordinator will update the Master Audit Schedule (MAS) (i060101) accordingly.

5.0 CONDUCTING THE AUDIT

Access to STEPS' systems and networks is securely managed through ISO 27001:2022 certification requirements. All audits require an Opening, Closing and Audit Review Meeting. The Opening meeting is where the Auditor will confirm the scope of the audit and the objective and timing of processes to be conducted. The Closing meeting will provide an overview of the findings of the audit, identify major and/or minor non-conformances and observations, advise the date the Audit Report will be received and any further requirements. Where Observations and / or Minor Non-conformances are raised as a result of the audit the Quality Assurance & Document Control Coordinator will schedule a series of monthly meetings with all impacted internal stakeholders to track progress of corrective actions to completion. These meetings will be scheduled fortnightly when Major Non-conformances are raised.

5.1 ONSITE AUDITS

Audits being conducted on STEPS' premises are required to be managed in accordance with STEPS ISO 27001:2022 certification. Auditors are required to:

- complete the Contractor Deed of Confidentiality (i030106)
- provide an Insurance Certificate of Currency for Professional Indemnity

Upon confirmation of the audit date the Quality Assurance & Document Control Coordinator will:

- book meeting room/s for the duration of the audit including the Opening and Closing Meetings
- using 'MS Teams' invite the Managing Director (MD) or Chief Executive Officer (CEO), department/program Manager and key staff to attend the specific audit sessions
- provide the MD, CEO, department/program Manager and key staff with the audit plan/schedule.

STEPS employees required to participate in the audit are identified by the department/program Manager responsible or the area being audited. Wherever possible, the Quality Assurance & Document Control Coordinator will provide at least six weeks' notice to required staff of an upcoming audit.

5.2 REMOTE/DESKTOP AUDITS

STEPS preferred platform for remote audits is via 'MS Teams'. Auditors are not permitted to remotely access STEPS' systems or network.

Audit documentation and/or evidence is uploaded to either an auditor portal or STEPS Audit SharePoint Folder. Where a STEPS Audit SharePoint folder is required, the Quality Assurance & Document Control Coordinator will endeavour to provide two weeks' notice prior to the audit for STEPS ICT department to create a specific Audit SharePoint folder, to which all documentary evidence will be uploaded.

Access to the Audit SharePoint folder is provided to the Auditor, Risk and Compliance Manager, Quality Assurance & Document Control Coordinator, and the Quality Systems Administration Coordinator and identified key department/program staff.

5.3 AUDIT PREPARATION

The Quality Assurance and Document Control Coordinator is responsible for liaising with outsourced internal and external auditors throughout the audit process and will confirm the Audit plan/schedule and the process for uploading all required audit documents. Prior to the audit, the Quality Assurance & Document Control Coordinator will:

- develop a list of required documents and evidence and upload them to the dedicated audit portal
- advise the department/program Manager of the sampling method for choosing participants to consent to and meet with the auditor/s and/or have their file reviewed
- arrange any end of day meetings the auditor has requested (for audits longer than one day)
- book meeting room/s for the duration of the audit including the Opening and Closing Meetings
- invite key staff to attend the specific audit sessions using MS Teams and/or meeting rooms
- update the Consent form provided by the auditors [or use the Service Assessment/Review Consent (i060305)] with relevant dates, program name, contact person and phone number. The Consent form is to be emailed to the program/department Manager and key staff to provide to participants who are invited to participate in the audit by interview (face to face, online or via phone) or file review

- arrange a meeting of all internal stakeholders where required to ensure all parties have a clear understanding of their roles and responsibilities as well as an opportunity to clarify any areas of concern.

The auditor may also request additional documentation and evidence during the audit which the Quality Assurance & Document Control Coordinator will obtain and upload to the dedicated audit portal.

6.0 AUDIT FINDINGS

A Closing Meeting will be held at the end of the final day of audit for all outsourced internal and external audits, at which the auditor will provide an overview of the findings and explain any minor or major nonconformity and observations.

  - **Conformity** – the 'fulfilment of a requirement'. To conform means to meet or comply with requirements to the procedure or standard being audited. It is at the auditor's discretion whether they wish to specifically include conformities in the audit report.
  - **Minor Nonconformity** – the requirements of the procedure or standard being audited are not fully met, or the outcome is only partly effective
  - **Major Nonconformity** – the requirements of the procedure or standard being audited are not met, or the outcome is ineffective. Several related minor nonconformities also constitute a major nonconformity.
- **Observation** – an opportunity for improvement or positive feedback.

The auditor will advise when the final Audit Report will be received and any associated processes.

6.1 AUDIT REPORT

On receipt of the Audit Report, the Quality Assurance & Document Control Coordinator will schedule an Audit Review Meeting. The invitees to this meeting will include the MD or CEO, Risk and Compliance Manager, the department/program Manager and key staff of the department/program involved in the audit.

This meeting will be minuted by the Quality Assurance & Document Control Coordinator with the minutes filed under the specific Audit File in the 'O' Drive under Quality Management.

The Audit Review Meeting Agenda (i060304) will:

- Review and discuss the Audit Report and identify any areas where there is a dispute in the audit findings
- Create a Corrective Action Plan (or use the plan the auditors have provided) and assign tasks to specific staff member/s with agreed dates of completion ensuring the following timelines are considered:
  - Major Nonconformity – actions are to be completed within **one month** from the date of the Audit Review Meeting
  - Minor Nonconformity – actions are to be completed within **three months** from the date of the audit review Meeting.
- Confirm the next meeting date.

6.2 CORRECTIVE ACTIONS

Following the Audit Review Meeting, the Quality Assurance & Document Control Coordinator will distribute the Corrective Action Plan to required staff.

The Quality Assurance & Document Control Coordinator will raise a record in the relevant management operating system for each non-conformity. Where an observation is going to be implemented, a separate record will be raised. Key information to be included in the record are:

- date of audit
- auditor's name and their company name
- department/program audited
- the non-conformance finding
- document name and number to be updated and/or developed (where relevant)
- corrective action owner and due date.

6.3 RECORDING & FILING

The Quality Assurance & Document Control Coordinator will:

- enter the date the audit report was received and update the status of the audit on the Master Audit Schedule (MAS) (i060101)
- file all audit documentation including the Audit plan/schedule, Audit Report and Corrective Action Plan into the specific audit folder in the 'O' Drive.

A summary of all Audit Reports will be included with the Quality Assurance and Risk Monthly Board Report.

Where agreed corrective actions are not completed within the required time frames, the Quality Assurance and Risk Manager will report this to the Executive Leadership Team (ELT).

7.0 RELATED DOCUMENTS

Document Name	Document Name
Acceptable Use Policy (6001700)	Audit Findings and Report (i060302)
Audit Review Meeting Agenda (i060304)	Contractor Deed of Confidentiality (i030106)
Financial Management (e310200)	Guest Access Procedure (6000500)
Master Audit Schedule (MAS) (i060101) *(Refer to the Quality Assurance & Risk team)*	Service Assessment/Review Consent (i060305)

8.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	25 July 2024
Effective Date	31 July 2024	**Document Number**	i060300_v9_240731

(Uncontrolled when printed)

1.11.2 Document Control

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) is committed to providing sufficient documented information (policies, procedures and associated documents) to demonstrate the effective planning, operation and control of its processes and the implementation and continual improvement of its Quality Management System (QMS). STEPS QMS contains all documented information for the STEPS Quality Manual (SQM) and Moodle, with Moodle containing documented information relevant to the delivery of training.

By documenting information, STEPS aims to:

1. communicate information
2. provide evidence of conformity (meaning that what was planned is being done)
3. share knowledge.

The SQM includes:

- **STEPS Organisational Policies & Procedures** contains information for the operation of processes throughout the organisation.
- **Service Stream** sections contain specific information on the programs STEPS operate.
- **Reference Documents** apply to the whole organisation and includes 'How To' guides and insurance certificates.

1.1 DEFINITIONS

Documents within the STEPS QMS are identified as:

Policies	Policy statements are derived from STEPS' commitment and values outlining goals and undertakings relevant to STEPS' overall vision and objectives.
Procedures	A procedure details a process by describing who, what, where, when and why. Procedures allow conformity against planned processes to be determined through audits.
Document Number	The unique number assigned to each document and located in the footer for policies and forms and in the governance table for procedures. All documents part of the document control system is identifiable by a document number.
Version	All controlled documents will be issued the next successive whole number for a new version.
Effective Date or Quality Load Date	The date from when document is effective and published. This is also known as the quality load date in the Document Register (i020201)
Document Register (i020201)	Register in where all controlled documents are recorded and assigned document numbers. The Document Register (i020201) is in G drive (G: \Quality Manual\STEPS_Navigator_Source_Documents\06_Document_Registers) and contains both current and approved versions, archived or pending.

Forms	A preformatted document with the provision for data entry to monitor progress. Once a form is complete it becomes a record.
‘How to’ Guides and Work Instructions	Provides step by step instructions on a specific task.
Live Documents	“Live” Documents are displayed on the SQM and contain shared information which is updated frequently. Version control is applied to the template only, e.g. Incident Register (5000050).
Quality Systems Administration Coordinator	Nominated STEPS employee who maintains the QMS to ensure documents comply with QMS requirements, or another member of the Quality Assurance and Risk team. Hereafter referred to QSAC.
OSI	Organisational System Improvement (Corrective Action Register) also known as OSI. This is the system STEPS uses for managing continual improvement with recording of non-conformances from internal and external audits and recording of complaints. OSI forms part of the document control system where documents are updated, approved and version controlled.

2.0 DETERMINING THE NEED FOR DOCUMENTED INFORMATION

Analysis of processes should be the driving force for defining the amount of documented information needed for the QMS. It should not be the documented information that drives the processes.

In general, most managers will be required to develop procedures and associated forms relevant to all or part of a program, contract or the area they are responsible for.

The manager responsible for developing procedures and associated forms will be the document owner.

It is the responsibility of the document owner to check the content of the proposed document/s to confirm compliance with legislation, relevant standards and contracts and that the accuracy and intended meaning is clear and concise.

The document owner is responsible for gaining approval of the document as per section 2.3.

Once approved, new documents must be submitted to the Quality Systems Administrator Coordinator (QSAC) using the OSI system for inclusion in the SQM or Moodle.

2.1 WRITING A PROCEDURE

When drafting a procedure, use the relevant Service Stream or programs ‘Procedure’ template located in the Digital Stationery Suite which can be accessed when opening a New document in Microsoft Office Word and clicking on *STEPS Group Australia Limited*. Refer to Access your Digital Stationery (365 or Citrix) (r400003) for detailed instructions.

The document owner will consider the following components when writing a procedure:

WHO will be using/referencing the procedure?	WHEN will the procedure be used?
WHAT will the procedure be used for?	WHY is the procedure necessary (i.e. which process is it supporting?)

WHERE will the procedure be used?	HOW will the procedure be used? (i.e. is this explained clearly in the content of the procedure?)

The document owner will prepare the draft document in the most appropriate format (e.g. electronic document; video, manual) so that the meaning and function are evident.

Employees with the authority to approve/authorise documents [refer to Delegations of Authority RACI Chart (i010602)] must check the content to confirm the accuracy and intended meaning or use is clear and concise.

Once approval has been obtained, the QSAC will ensure the document complies with the organisational styles and branding requirements, update the Document Register (i020201), apply version control information and upload the document to SQM or Moodle.

Where appropriate, the relevant manager/supervisor will advise their team of the new procedure or form relating to the procedure and arrange for training of relevant personnel in the use of the procedure or form relating to the procedure.

Where an electronic version of the new document is not available, a hard copy of the new document needs to be issued.

2.2 AMENDMENTS TO EXISTING DOCUMENTS

An application for review, or an amendment of any existing approved document must be made using the OSI system. QSAC will determine the most appropriate Responsible Person (RP) for any OSI raised. The RP will ascertain whether the amendment is warranted, confirm the accuracy and intended meaning is clear and concise and provide evidence of approval for the amended document.

Once approval has been received by the QSAC via the OSI system, the document will be loaded into the QMS and released for use.

2.3 AUTHORISATIONS AND APPROVAL

All Organisational Policies and Procedures must be approved by STEPS Policies & Procedures Sub-Committee who meet regularly (usually fortnightly).

The Chair of STEPS Policies & Procedures Sub-Committee will be assigned RP for the OSI.

The Delegations of Authority RACI Chart (i010602) indicates which positions have the authority to approve controlled documentation.

3.0 DOCUMENT NUMBERING AND FORMAT

STEPS controls documented information to ensure:

- documents are approved for adequacy and legibility
- reviews and updates are processed through the OSI system to demonstrate continual improvement
- version control is applied to ensure documents are current and prevents the use of superseded or obsolete documents.

Each document has been assigned a unique number as part of the document control process. All controlled documents are identifiable by a document number. If a document number has changed, the previous document number can be referred to in the Document Register (i020201) field named *Previous ID #*. The document number is in the footer for policies and forms and in the governance table for procedures. All policies and procedures have notation that a document is uncontrolled once printed to assist in preventing the use of superseded or obsolete documents.

Controlled documents will be issued the next successive whole number for a new version. Documents that are controlled will have a unique document number, version number and effective date displayed in the document. Please note:

- A shortened version of the document numbers is displayed in documents (unique number_ version number_effective date) and is the name given to files saved in G:\Quality Manual\STEPS_Navigator_Uploads\SN\FD.
    - Format of shortened version number: DocumentNumber_VersionNumber_EffectiveDate
- The whole document number (not shortened) is recorded in the Document Register (i020201) as well as the file names of documents saved in G:\Quality Manual\STEPS_Navigator_Source_Documents. The format of whole document numbers is:
        - FunctionalArea_DocumentNumber_Abbreviation_VersionNumber_EffectiveDate_OSInumber
- The effective date displays in the format yymmdd.

The document numbering format is based on document type (being a procedure or a document), which functional area/program, and which "parent" document it relates to.

Documents associated with a "parent" document are numbered from the "parent" document number. The numbering associated with a parent document is:

- "Parent" document: **iAAXXZZ** (Example: i051000)
    - **i** represent that the document is associated with Organisational Policies and Procedures
        - both "i" or "e" at the start of the document number signifies that the document is associated with Organisational Policies and Procedures. All other functional area or programs document number is by the format AAXXZZ (no "i" or "e" or other letter included).
    - **AA** indicates the functional area or program/stream. This number represents the highest-level grouping and details about specific numbers are detailed in Version Control Numbering System (i020204) In the Document Register (i020201), this number is recorded in the field *Chapter*.
    - **XX** indicates which consecutive procedure the document relates to. Each new procedure that is added in a specific functional area or program, will be assigned the next available successive number. In the Document Register (i020201), this number is recorded in the field *Procedure* and starts with 00. This means that each procedure within a functional area or program will have a different number recorded in the field *Procedure*.
        - 00 recorded in the field *Procedure* signifies the document is not related to a procedure and may be an orphan document.
        - 01 recorded in the field *Procedure* may signify the document is a policy.
        - 10 in above example indicates this is the 10th procedure added to the functional area 05.
    - **ZZ** indicates which consecutive related document or form that relates to the procedure as indicated in the field *Procedure*. In the Document Register (i020201), this number is recorded in the field *Form/Doc#* and starts with 00.
        - When the document type is a procedure, the **ZZ** number is usually 00.

Examples of document numbering:

- The first procedure of Maintenance of Pool Vehicles (i051000) was issued as:

  - i051000_v1_160905 (short document number) and IMS_i051000_MainPoolVehic_v1_160905_3411 (whole document number)
- The first form required for this procedure had the document number i051001_v1_160609 (short document number) and IMS_i051001_MVInsp_v1_160609_3302 (whole document number)

In above examples:

- i05 refers to the functional area or program
- 10 refers to which procedure number
- 00 refers to document type being a procedure or if 01 or higher means the sequential form associated with the procedure that has been issued

In addition to the above numbering rules, depending on what functional area or program the document is associated with, the following numbering should be applied to the *Procedure* field in the Document Register (i020201):

Functional area or Program	Procedure Field Number to use	Document types as signified by the procedure number
AMEP	0	Ops Forms
AMEP	1	Accredited Resources
AMEP	2	Policies
DES	90	Forms and Resources
DES	80	Work Instructions
DES	70	YouTube
SEE	1	Non-Accredited
SEE	2	PTA
SEE	3	IPA
SEE	4	Accredited

Signed Training and Assessment Strategies (TAS') for individual courses have further version control applied so the TAS template of which the signed TAS is based on can be identified. The signed TAS must have the following additional data entry applied in the Document Register (i020201):

- Update the field *TAS Version Control Footer - when applicable* with the related TAS template version footer in the format 1500701_v#_yymmdd.

Here is an example of what must be copied from the document register into the signed TAS:

Based on Training and Assessment Strategy Template 1500701_v7_230420

1280001_v1_230421

Use the fields named *TAS additional version footer – when applicable* and *Version Control – Footer* in the Document Register (i020201) to copy the required version control information into the signed TAS footer.

When the TAS template is updated, all related signed TAS' must be updated using the new template.

Document number will be applied prior to publication in the SQM and Moodle by the QSAC using the Document Register (i020201) located in G:\Quality Manual\STEPS_Navigator_Source_Documents\06_Document_Registers.

The Document Register (i020201) contains several fields which are detailed in the Glossary for the Document Register (i020203).

4.0 DISTRIBUTION

Most documents are available electronically on the SQM and in Moodle with access available via the STEPS server. Other types of information such as video can be included in STEPS documented information.

Selected chapters on the SQM can be supplied via a user manual in PDF format which can be printed and shared. The following user manuals are available on https://www.stepsgroup.com.au/staff-portal/ and updated monthly by the QSAC:

- NDIS Policies and Procedures
- COVID-19 Manual
- STEPS Organisational Policies and Procedures.

Detailed instructions on how to download the PDF user manuals from the website is explained in Access NDIS and STEPS Organisational Policies and Procedures via the Internet (r400051). Due to being updated monthly, the PDF user manuals could be delayed in showing the latest versions.

To be able to publish the SQM into a PDF user manual, the relevant chapters must be setup in HTML format (not only a link to a file in FD). Technical documentation on how to update the SQM with HTML can be accessed on https://www.helpandmanual.com/help/index.html.

The published PDF files are kept in the folder as source documents G:\Quality Manual\STEPS_Navigator_Graphics\PDF Publishing.

PDF user manual can also be used for audit purposes to be able to supply a printable copy of the SQM to external auditors.

Chapters that must have all the procedures setup in HTML format includes:

- STEPS Organisational Policies and Procedures (and all sub chapters)
- COVID-19 (and all sub chapters)
- Social Business – STEPS Pathways College (sub-chapter only)
- NDIS (National Disability Insurance Scheme) (and all sub chapters).

5.0 STORAGE AND PRESERVATION

STEPS' documented information is stored securely in the Quality Manual on the G: drive where access is restricted to the Quality Assurance & Risk team. This ensures that documents are protected from unauthorised changes or loss.

It is the responsibility of each employee to ensure that they are accessing documented information through either the SQM or Moodle. No copies of documents should be stored in O: or H: drives or on individual desktops.

6.0 ARCHIVING OR OBSOLETING

Superseded and obsolete documents are archived in the functional area or program relevant archive folders located in the Quality Manual G: drive and all files are backed up in accordance with the Backup Policy (6002000).

Details about archiving different document types in G drive and Help and Manual are explained in Document Replacing and Archiving Process (i020202).

7.0 RELATED DOCUMENTS

Document Name	Document Name
Access NDIS and STEPS Organisational Policies and Procedures via the Internet (r400051)	Access your Digital Stationery (365 or Citrix) (r400003)
Backup Policy (6002000)	Delegations of Authority RACI Chart (i010602)
Document Register (i020201) Maintained by the Quality Assurance & Risk Team in G:\Quality Manual\STEPS_Navigator_Source_Documents\06_Document_Registers	Document Replacing and Archiving Process (i020202)
Glossary for the Document Register (i020203) Maintained by the Quality Assurance & Risk Team in G:\Quality Manual\STEPS_Navigator_Source_Documents\06_Document_Registers	Version Control Numbering System (i020204) Maintained by the Quality Assurance & Risk Team in G:\Quality Manual\STEPS_Navigator_Source_Documents\06_Document_Registers

8.0 GOVERNANCE

Document Owner	Manager – Quality Assurance & Risk	**Approval Date**	13 July 2023
Effective Date	14 July 2023	**Document Number**	i020200_v5_230714

(Uncontrolled when printed)

1.11.3 Monitoring Quality Management System Performance

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has identified the importance of the establishment and maintenance of a quality management system that supports the various functions and process used throughout the organization in the delivery of services. STEPS recognises the crucial role that the Managing Director, the Board and the Executive Leadership Team (ELT) have in driving quality management and the importance of leadership commitment to quality management principles that assist the organisation in achieving its goals in the wider marketplace in which it operates.

This procedure sets out the requirements for monitoring quality management system performance across all STEPS Group of Companies (STEPS) workplaces and activities.

1.1 MONITORING IMPLEMENTATION OF OBJECTIVES AND TARGETS

A review of the stated quality objectives will be reported in intervals as stated in the Quality Objectives Plan (i010301). A monthly quality performance report detailing review findings will be forwarded to the Board to enable full discussion of outstanding items and resources (financial, time and personnel), to be allocated to implement each outstanding objective and to report back to Managing Director and the Board on progress.

Actions determine by the ELT will be forwarded to the appropriate manager who will discuss actions at meetings to ensure that all managers and workers are aware of the objectives that apply to their area of control and the strategies that may be undertaken to achieve the targets set by ELT.

1.2 MONITORING OF THE QUALITY MANAGEMENT SYSTEM THROUGH AUDITS

STEPS has established an audit programme for the business to monitor continuous improvement of WHS, quality and environment management practices across the whole of the organisation.

The audit scope encompasses those areas critical to the business and follows the Plan, Do, Check, Act (PDCA) cycle of management with audits at pre-determined intervals:

- The audit program is pre-set yearly at executive meetings and recorded on the Master Audit Schedule (MAS - i060101).
- The documented audit schedule and criteria will be based on the significance of health and safety risks identified within the risk assessment process and previous audits.
- Audits will focus on:
    - system implementation and compliance.
    - the significance of risks including any results of previous audits.
    - review of previous audited items and non-conformances to ensure full closure. The audit process shall include measurement of:
- Quality management system objectives and their implementation.
- Monitoring health and safety, environment impacts and quality risks and the results of previous audits.
- The audit protocol will include both system and process compliance and be conducted by:
    - trained workers.
    - external audits conducted by third party organisations.

Completion of inspections will be one of the ‘targets’ which shall form part of the WHS Key Performance Indicators that are assessed monthly against relevant documentation and reported to ELT.

1.3 REPORTING

The following reporting data has been developed from the established objectives for key business areas. Monthly reports are compiled at the conclusion of review of objectives of the business and made available for the Board and ELT for review and feedback.

1.3.1 AUDIT REPORTING

Audits will be planned, conducted and recorded as documented in the Audits Procedure (i060300). The performance of audits as per the Master Audit Schedule (MAS - i060101) will be reported on and the corrective actions noted.

1.3.2 PERFORMANCE MEASUREMENT & SURVEYS

Performance measurement activity and survey updates is to be reported.

1.3.3 FEEDBACK AND COMPLAINT MONITORING

Details of complaints and feedback submitted between reports along with trend data are to be reported.

1.3.4 ORGANISATIONAL SYSTEM IMPROVEMENTS (OSI)

The OSI system remains the principal indicator of actions taken to continually improve the effectiveness of the quality management system. OSI’s include continual improvement actions documented and captured in the system and the responses taken to:

- Non-conforming processes and observations made during audits.
- Complaints.
- Changes and development of new documents.
- Low risk rectifications of hazards; and
- Management review.

Report detailing OSI’s raised by category (i.e. audit, change in SQM and complaints) and identifying the service streams is compiled.

1.3.5 RISK MANAGEMENT

The status of the Risk Management activity and plans is to be included.

1.3.6 LEGISLATIVE CHANGES

Legislative changes between reports is provided and the Legislative Register (i020101) is maintained.

2.0 RELATED DOCUMENTS

Document Name	Document Name
Audits Procedure (i060300)	Legislative Register (i020101)
Master Audit Schedule (MAS - i060101)	Quality Objectives Plan (i010301)

3.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	5 June 2023	**Document Number**	i060100_v2_230602

(Uncontrolled when printed)

1.11.4 Organisational System Improvement (Corrective Action Register)

1.0 IMPROVEMENT OF PRODUCT AND SERVICES

Improvement of product and services will be managed in accordance with this procedure.

STEPS Group of Companies (STEPS) shall implement the necessary actions to meet customer requirements and enhance customer satisfaction. This will include improving processes and systems:

- to prevent non-conformities through the use of internal audits and responding to feedback from customers.
- to meet known and predicted requirements by ensuring documented procedures meet contract requirements and are current and accessible to staff.

Actions will be recorded on the Organisational System Improvement (OSI) system.

2.0 SUPPORTING THE CONTINUAL IMPROVEMENT PROCESS

The continual improvement process is supported through the use of the OSI system. This system allows for the input of complaints; audit findings and any actions taken to improve processes through changes to policies, procedures and forms.

3.0 MANAGING THE OSI PROCESS

The Quality Assurance & Risk team are responsible for the administration processes to progress the OSI through the five separate phases:-

1. Raising an OSI
2. Assigning an OSI
3. Approving an OSI
4. Processing an OSI
5. Closing an OSI

4.0 RAISING AN OSI

- Any employee of STEPS can raise an OSI
- The employee who raises an OSI is known as the ‘Initiator’. The OSI Process Workflow (i060401) provides an overview of the Initiator and Quality Assurance & Risk team’s associated actions.

5.0 ASSIGNING AN OSI

- Each OSI is assigned to a ‘Responsible Person’ (RP).
- All STEPS Policies and Procedures require the approval of the Policy & Procedure Subcommittee and the Board of Directors.
- All operational procedure changes can be approved by the relevant Executive Manager.
- If the RP has not completed the ‘Approve OSI for Closure’ section within six months of the OSI submission date, the OSI will be closed. However, the exception is any OSIs that are categorised as an Audit Finding, not approved within the six-month time frame by the relevant RP, will not be automatically closed. Any OSIs categorised as Audit Finding not actioned within this time, will be escalated to the Quality & Risk Subcommittee.’ For all other OSIs, the RP will receive one notification from the Quality Assurance & Risk Team that the OSI is overdue advising if not approved the OSI will be closed. If the OSI is still relevant, a new OSI is to be raised by the RP.
- Where a form is submitted which does not relate to an existing procedure or workflow, the form will be returned to the ‘Initiator’ with the notification that a procedure or workflow must be developed which outlines the use of the form.
- When assigning OSIs these are assigned as low risk rating. Where a hazard or risk is identified, refer to the Risk Management Procedure (i050100).

The Quality Systems Administration Coordinator will action and assign OSIs using one of the following categories:

- **Assessment Validation** – OSIs will be assigned to the Manager responsible for the processes validated.
- **Audit** – OSIs will be assigned to the Manager responsible for the area or processes audited.
- **Document Review** – All new and existing changes to Corrections and changes with no operational impact will be assigned and actioned by the Quality Assurance & Risk team. The Quality Assurance & Risk team will seek clarification and approval from the relevant manager as identified in the Delegation of Authority RACI Chart (i010602) for all other changes.
- **Document – new** – Will be assigned to the Executive Leadership Team (ELT) Member listed as the document owner.
- **Document – change/update** – Will be assigned to the Executive Leadership Team (ELT) Member listed as the document owner.
- **Customer Complaints** – Will be assigned in accordance with the Feedback and Complaints Policy (i010103).

6.0 COLLATING OSI DOCUMENTATION

The Quality Systems Administration Coordinator collates policies and procedures and their related documents submitted through the OSI System that require approval by the Policy & Procedure Subcommittee.

These documents are saved to O: Drive> Drafts>P for PP Committee. The documents are forwarded to the Executive Administration Manager every fortnight, three days prior to the Policy & Procedure Subcommittee meeting.

7.0 APPROVING AN OSI

STEPS Policy & Procedure Subcommittee are responsible for reviewing and approving STEPS Group organisational new and updated policies, procedures and their related documents raised in the OSI.

All individual business stream new and updated policies, procedures and their related documents are tabled at the first monthly meeting of the Executive Leadership Team (ELT).

7.1 APPROVAL OF POLICIES

Following approval by the Policy & Procedures Subcommittee, all policies are then tabled at the next Board Meeting for approval.

8.0 PROCESSING AN OSI

All OSIs are processed by the Quality Assurance & Risk team within five days from notification of approval by the Chair of the Policy & Procedure Subcommittee.

All OSIs that are uploaded to the SQM/Moodle and can be viewed on the OSI Reports section of the OSI System.

9.0 CLOSING AN OSI

A summary of actions and/or reasons for decisions will be provided to the initiator who will indicate if they are satisfied with the outcome.

INITIATOR SATISFIED WITH THE OUTCOME OF THE OSI

The Initiator will: -

- review the actions completed.
- tick the box to indicate they are satisfied; this will then close the OSI.

Where the ‘Initiator’ is not satisfied with the outcome of the OSI, the Quality Systems Administration Coordinator will review their comments and action as required using his/her discretion to close the OSI or contact the RP for further consideration.

INITIATOR NOT SATISFIED WITH THE OUTCOME OF THE OSI

Where the ‘Initiator’ is not satisfied with the outcome of the OSI:-

- they don’t tick the box to indicate they are satisfied.
- write the reason why they are not satisfied in the comment section. A member of the Quality Assurance & Risk team will contact the Initiator to discuss further.

Where an ‘Initiator’ has not responded to the request to close an OSI, the Quality Systems Administration Coordinator will: -

- send one OSI Closure Email Notification reminder to the ‘Initiator’ to close the OSI.

- If the ‘Initiator’ has not responded to the OSI Closure Email Notification reminder, the Quality Systems Administration Coordinator will call the Initiator requesting they close the OSI.

The Quality Assurance & Risk team has the authority to close OSIs where:

- If the ‘Initiator’ fails to close the OSI prior to the next month’s OSI data report, the Quality Systems Administration Coordinator will close the OSI.
- The ‘Initiator’ has left the organisation.
- A complaint has been indicated as resolved.
- Extenuating circumstances (as determined by the Quality Assurance & Risk team) prevent the ‘Initiator’ from closing an OSI.
- Duplicate OSIs have been raised.

10.0 REPORTING CONTINUAL IMPROVEMENT ACTIVITY

To facilitate the actioning and closing of OSIs, the Quality Assurance & Risk team will provide a follow up email and/or phone contact to the RP or Initiator to review and action any outstanding OSIs.

Continual improvement activity will be reported monthly to the Board and ELT.

Reports containing completed and published OSIs, are available on the STEPS Intranet under the 'OSI' tab and can be filtered by date range.

Managers will ensure that OSI reports are a permanent agenda item and discussed at all Team Meetings. Minutes are required confirming that both the STEPS Group Australia and if applicable their Service Stream OSI reports have been discussed. The minutes will act as a training record confirming which employees have been informed of relevant changes and to meet compliance requirements. The Agenda and Minutes should be recorded on the Meeting Agenda / Minutes Template (i040401).

11.0 RELATED DOCUMENTS

Document Name	Document Name
Complaints Procedure (i040500)	Delegations Register (i010601)
Effective Meetings (i040400)	Feedback and Complaints Policy (i010103)
Feedback Procedure (i040100)	Meeting Agenda / Minutes Template (i040401)
OSI Process Workflow (i060401)	Risk Management Procedure (i050100)

12.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 December 2022
Effective Date	12 December 2022	**Document Number**	i060400_v8_221212

(Uncontrolled when printed)

1.11.5 Quality Objectives

1.0 QUALITY SYSTEM OBJECTIVES

The Quality Objectives Plan (i010301) is used to document the quality objectives for STEPS Group of Companies (STEPS). It includes various functions and processes used throughout the organisation and in the STEPS Quality Manual (SQM).

The Quality Objectives Plan (i010301) describes functions and processes used by STEPS to:

- Support the Quality Policy (i010111),
- Enhance customer satisfaction, and
- Identify non-conformities.

Each of these functions and processes identifies who is responsible for what needs to be done, how it will be done, when it will be completed and how results are to be reported.

1.1 CHANGING QUALITY OBJECTIVES

Any changes to the quality system shall be planned and recorded on the Quality Objectives Plan (i010301) to ensure the purpose of the change is recorded and potential consequences understood. This planning process will assist to maintain the integrity of the quality system, ensure the availability of resources and allocate responsibilities and authorities.

2.0 MONITORING AND APPROVING THE QUALITY OBJECTIVES

The Quality Objectives Plan (i010301) will be approved by the Executive Leadership Team (ELT) by August each year and a report will be provided on the continued suitability and applicability of the Quality Objectives each July.

3.0 RELATED DOCUMENTS

Document Name	Document Name
Quality Objectives Plan (i010301)	Quality Policy (i010111)

4.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 June 2023
Effective Date	2 June 2023	**Document Number**	i010300_v3_230602

(Uncontrolled when printed)

1.11.6 Records Management Archiving

1.0 INTRODUCTION

Records management is an organisational function devoted to the management of information throughout its life cycle – from creation to disposal. The records management function is managed by the Quality Assurance & Risk Team. STEPS is required to maintain effective records management and information systems to meet legal and contractual requirements.

1.1 DEFINITIONS

Grace RS Web	Grace Records System Website
GRM	Grace Records Management

2.0 SYSTEMS

We have an agreement with Grace Records Management (GRM) whose services include:

- Supply of archive boxes and barcode labels
- Storage of archived documents
- Pickup and retrieval of archived files to and from office to the offsite Grace storage facility

Archived files are also recorded in the GRM system using the Grace RS Web.

We have the following Grace accounts:

- STEPS - Shared Services
- STEPS - Townsville
- STEPS - Cairns
- STEPS - Darwin
- STEPS - ICT
- STEPS - Social & Community
- STEPS - Casuarina
- STEPS – Hobart

The File Management Register is used by the Quality Assurance & Risk Team to record current and archived files. (O:\Quality Management\2725_Records Management\FileManagementRegister.xlsx)

3.0 FILE CREATION

Send an email to the Quality Team Inbox (qualityteam@stepsgroup.com.au) requesting creation of a new file (hard copy, electronic or both), providing the file name and schedule code. Refer to the File Structure (i020304) for Schedule Codes for your department.

4.0 ORDERING MATERIALS FROM GRM

Archive boxes and barcodes can be ordered on the Grace RS Web. If access is required to the Grace RS Web, email the Quality Team Inbox. GRM will only accept GRM archive boxes.

5.0 SENDING ARCHIVED RECORDS TO A GRM FACILITY

Once a record is no longer required for current use, records will be archived in line with contractual and legislative requirements. All paper-based records must be archived and recorded in the GRM.

STEPS sites with an existing Grace RS Web user login can arrange to have their records stored offsite by booking a pickup through the Grace RS Web. GRM will collect boxes from designated STEPS sites and store on their premises.

Important:

The Archive Box Contents (i020305) must be completed and forwarded to the Quality Team Inbox prior to the archived documents being despatched to GRM offsite storage. The Quality Systems Administration Coordinator will record the archive box barcode, file name and retention dates for each box in Grace RS Web and in the File Management Register.

STEPS sites who have not stored archived records at a GRM facility previously must contact the Quality Systems Administration Coordinator to arrange the setup of a Grace RS Web account.

6.0 RETRIEVAL OF ARCHIVED RECORDS

To request retrieval of archived records, email the Quality Team Inbox. The Quality Systems Administration Coordinator will then record this request on the Records Retrieval Register (i020301) and retrieve the requested records.

7.0 DISPOSAL OF RECORDS

To ensure effective control of non-current records, disposal will be undertaken when records have met their minimum retention period in line with contractual and legislative requirements.

The Quality Systems Administration Coordinator will organise Box Content Reports which will be extracted from Grace RS Web every 12 months to identify non-current records which are eligible for destruction.

Once records have been identified for destruction, the Quality Systems Administration Coordinator will provide the responsible Executive Leadership Team (ELT) member with:

- Record Disposal Authorisation Form (i020302)
- Box Contents Report (GRM)

The Record Disposal Authorisation Form (i020302) requires approval by the relevant ELT Member, which is then to be authorised by the Managing Director. If a record is deemed to be ineligible for destruction, this needs to be recorded on the Record Disposal Authorisation Form (i020302).

The Record Disposal Authorisation Form (i020302) is to be returned to the Quality Systems Administration Coordinator who will update RS Web indicating a review date or permanent retention for records that are ineligible for destruction.

The Quality Systems Administration Coordinator is to forward a barcode list of records that have been authorised to be destroyed to GRM via email. (There is not an option to complete this function using Grace RS Web).

GRM will create a Pre-Work order and forward a Confirmation of Certificate of Destruction to STEPS. GRM will issue the Confirmation of Destruction no later than two days after they receive the barcode list. The Certificate of Destruction is then to be signed by the Managing Director of STEPS and returned to GRM.

Once GRM receives the signed Confirmation of Destruction, they will proceed to destroy the boxes. Grace RS Web is automatically updated once the records are pulled from the shelf to be destroyed.

A Certificate of Destruction is sent to STEPS up to six weeks after destruction. Archive boxes are pulled at the start of the month at GRM facilities to allow 'cancel destruction' in case of emergency.

The Quality Systems Administration Coordinator will update the Records Disposal Register (i020303) and all documentation will be filed.

7.1 DISPOSAL OF EDUCATION & TRAINING DOCUMENTATION

Education & Training documentary evidence is archived in accordance with the guidelines of the specific course/program contract or agreement and the Australian Skills Quality Authority (ASQA) Standards for Registered Training Organisation (RTO) 2015, these timeframes are noted below:

• Adult Migrant English Program (AMEP)	7 years
• Employability Skills Training (EST)	10 years
• Registered Training Organisation (RTO)	30 years
• Skills for Education and Employment Program (SEE)	10 years
• Skills Assure Supplier	7 years

7.2 DISPOSAL OF HARD STUDENT DOCUMENTS

Refer to STEPS Education & Training Procedures:

C3G - Destruction of Hard Copy Student Documents Procedure (1140121)

SQW – Destruction of Hard Copy Student Documents Procedure (1170120)

Skills Tasmania – Destruction of Hard Copy Student Documents Procedure (118200)

7.3 EMPLOYEE RECORDS

Employee Records are required to be kept for a period of seven years. Refer to Record-keeping - Fair Work Ombudsman and Employee records | business.gov.au for Employee Record disposal guidelines.

8.0 ELECTRONIC RECORDS

Electronic records are backed up in accordance with the STEPS Group of Companies Backup Policy (6002000).

9.0 RELATED DOCUMENTS

Document Name	Document Name
Archive Box Contents (i020305)	Backup Policy (6002000)
C3G - Destruction of Hard Copy Student Documents Procedure (1140121)	Data Classification Procedure (6000300)
File Management Register *Refer to Quality Assurance & Risk Team*	File Structure (i020304)
Record Disposal Authorisation Form (i020302)	Records Disposal Register (i020303) *Refer to Quality Assurance & Risk Team*
Records Retrieval Register (i020301) *Refer to Quality Assurance & Risk Team*	Skills Tasmania – Destruction of Hard Copy Student Documents Procedure (118200)
SQW – Destruction of Hard Copy Student Documents Procedure (1170120**)**	

10.0 GOVERNANCE

Document Owner	Chief Administrative Officer	**Approval Date**	1 December 2022
Effective Date	5 December 2022	**Document Number**	i020300_v5_221205

(Uncontrolled when printed)

1.12 Feedback and Complaints

Enter topic text here.

1.12.1 Feedback

1.0 MANAGING FEEDBACK

This procedure establishes an effective and consistent framework for the management of feedback for STEPS Group of Companies (STEPS) services, activities, systems, and processes to support continuous improvement. Quality is ultimately determined by customers; therefore, it is critical we encourage their feedback which includes complaints, compliments, concerns, and suggestions all of which provide opportunities for improvement. If you need to process and manage a complaint, refer to the Complaints Procedure (i040500).

The principles of natural justice and procedural fairness underpin this Feedback Procedure (i040100). We will support customers to access advocacy and/or bilingual support.

1.1 DEFINITIONS

Feedback	Feedback includes complaints, concerns, compliments, and suggestions for improvement about a particular service, experience, or event - not simply a statement of overall opinion about STEPS services.
Complaint	Expression of dissatisfaction made to STEPS, related to its products (including services), or the complaints handling process itself, where a response or resolution is explicitly or implicitly expected. A complaint is not: • a request for information or explanation of policies; or • a disagreement with a decision that has a formal avenue of appeal. Where no contact details are provided, the complaint will be treated as feedback. The above definition is consistent with Australian Standard ISO 10002-2018.
Customer	Any person or business who receives products or services from STEPS including students, participants, and jobseekers.
Stakeholder	All those who have a stake/interest in STEPS e.g., government, schools, employers.

2.0 GENERAL

2.1 ENCOURAGING FEEDBACK

Feedback from our customers and stakeholders is valued and customers are encouraged to voice their opinions on any aspect of service provision, including:

- Complaints
- Compliments
- Concerns
- Suggestions.

Customers and stakeholders are to be informed that any feedback provided to STEPS will be making a positive contribution towards assisting us improve our services. When the feedback is a complaint, it will be processed and managed according to the Complaints Procedure (i040500).

In recognition of the special needs of some customers and stakeholders (for example those from culturally and linguistically diverse backgrounds, those who speak another language or those who have a cognitive or physical impairment) feedback can be raised on their behalf by their nominated advocate.

A Feedback Box and a supply of Tell Us What You Think (i040102) forms are available at each STEPS site that delivers a service to our customers and are accompanied by a Feedback Box Explanatory Statement (i040103).

2.2 PROCESS FOR PROVIDING FEEDBACK

Customers and stakeholders can provide feedback using one of the following methods:

- Tell Us What You Think (i040102) form
- Via email to cso@stepsgroup.com.au
- Via STEPS website ‘Contact Us'
- By Letter mailed to PO Box 1139, CALOUNDRA QLD 4551
- Face-to-face with a member of staff
- Through a phone call to a manager or coordinator
- Through a phone call to the STEPS Customer Service Officer (CSO) on (07) 5458 3000.

Workers must record verbal feedback on a Tell Us What You Think (i040102) form or by using the *Feedback and Complaint Outlook Form* which can be found in the Organisational Forms Library located in Outlook:

- Click on New Items under the Home ribbon
- In dropdown, click More Items and then Choose Form
- In the Choose Form window, select Organisation Forms Library, then double-click on Feedback and Complaint and the *Feedback and Complaint Outlook Form* email will open ready to fill out.

Feedback can be made anonymously in line with the National Disability Insurance Scheme (Complaints Management and Resolution) Rules 2018.

Any of the above methods can be used by a customer’s nominated advocate.

2.3 INFORMING CUSTOMERS

On entry to a service, all customers receive an information booklet relevant to the Service Stream.

The booklet includes information on:

- Processes for providing feedback and raising complaints
- How to gain assistance to complete a Tell Us What You Think (i040102) form
- The customer’s right to access and be supported by an independent advocate of their choice

Reminders of the feedback process should be provided regularly to customers.

2.4 COLLECTION OF FEEDBACK

Any feedback received is forwarded to the relevant department/program manager.

It is the responsibility of the department / program manager to ensure all Tell Us What You Think (i040102) forms are collected and processed at the end of each week from the Feedback Box.

All feedback is to be sent to the Quality Assurance & Risk team either by:

- Scanning and emailing the completed forms to qualityteam@stepsgroup.com.au; or
- Emailing the *Feedback and Complaint Outlook Form* (refer to section 2.2 detailing where to find the *Feedback Outlook Form).*

2.5 RECORDING OF FEEDBACK

The Quality Assurance & Risk team will save all feedback forms received in the electronic folder located in the ‘O’ drive, naming the file as the corresponding Feedback ID number from the Feedback Register (i040106), e.g. “Feedback ID 232.pdf”.

The Quality Assurance & Risk team will record all feedback received in the Feedback Register (i040106) and analyse entries to identify and manage trends, and to recommend system improvements.

When feedback is sent directly to Corporate Services, the Risk and Compliance Manager will determine if acknowledgement of feedback is required. Where acknowledgement is required, the Risk and Compliance Manager or delegate will contact the customer.

Any actions taken in relation to the feedback will be recorded in the Feedback Register (i040106).

3.0 REPORTING

The Quality Assurance & Risk team will provide monthly summarised feedback reports through the Quality Assurance & Risk team Report which will be forwarded to the Executive Leadership Team (ELT) and Board of Directors.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Complaints Procedure (i040500)	Feedback Box Explanatory Statement (i040103)
Feedback and Complaints Policy (i010103)	Feedback Register (i040106) *Refer to the Quality Assurance & Risk team*
Feedback and Complaint Outlook Form *Refer to Outlook > New Items > More Forms > Choose Form > Organisational Forms Library > Feedback and Complaint*	Tell Us What You Think (i040102)

5.0 GOVERNANCE

Document Owner	Risk and Compliance Manager	**Approval Date**	23 May 2024
Effective Date	6 June 2024	**Document Number**	i040100_v11_240606

(Uncontrolled when printed)

1.12.2 Complaints

1.0 COMPLAINTS

This procedure establishes an effective and consistent framework for the management of complaints to ensure staff manage all customer complaints and appeals in a professional and timely manner to enhance the quality of service provided to our customers through STEPS Group of Companies (STEPS) services, activities, systems, and processes can be continually improved.

Quality is ultimately determined by customers; encouraging our customers to express their dissatisfaction is critical as complaints are an opportunity for improvement. Other feedback types including concerns, compliments and suggestions are also encouraged and are to be processed according to the Feedback Procedure (i040100).

Complaints sometimes relate to an incident that has occurred. In these instances, respond and investigate complaint as an incident. Refer to the Incident Management Procedure (i090700) if the incident relates to NDIS or Mental Health programs, otherwise process according to the WHS Incident Notification Procedure (i090200).

Complaints specifically relating to RTO assessment outcomes should be dealt with in accordance with the Assessment Appeals Procedure (1501800).

The principles of natural justice and procedural fairness underpin this Complaints Procedure (i040500). We will support customers to access advocacy and/or bilingual support.

1.1 DEFINITIONS

Complaint	Expression of dissatisfaction made to STEPS, related to its products (including services), or the complaints handling process itself, where a response or resolution is explicitly or implicitly expected. A complaint is not: • a request for information or explanation of policies; or • a disagreement with a decision that has a formal avenue of appeal. Where no contact details are provided, the complaint will be treated as feedback. The above definition is consistent with Australian Standard ISO 10002-2006.
Feedback	Feedback includes complaints, concerns, compliments, and suggestions for improvement about a particular service, experience, or event - not simply a statement of overall opinion about STEPS services.
Complainant	The individual raising a complaint.
Customer	Any person who receives products or services from STEPS including students, participants, and jobseekers.
Stakeholder	All those who have a stake/interest in STEPS e.g., government, schools, employers.

2.0 GENERAL

2.1 DEALING WITH COMPLAINTS

All workers in direct contact with customers and stakeholders have a responsibility to report any concerns or complaints in accordance with this procedure.

Customers and stakeholders are to be reassured that all complaints will be dealt with in a fair, prompt, and confidential manner, with no retributive action towards them as their complaints will be making a positive contribution towards assisting us improve our services.

In recognition of the special needs of some customers and stakeholders (for example those from culturally and linguistically diverse backgrounds, those who speak another language or those who have a cognitive or physical impairment) complaints can be raised on their behalf by their nominated advocate.

A colour copy of the Complaints Process (i040101) is displayed at all STEPS sites that deliver a service to our customers.

2.2 PROCESS FOR RAISING COMPLAINTS

Customers and stakeholders can raise complaints using one of the following methods:

- Tell Us What You Think form (i040102)
- Via email to cso@stepsgroup.com.au
- Via STEPS website www.stepsgroup.com.au
- By Letter
- Face-to-face with a member of staff
- Complaints can also be made anonymously
- Through a phone call to a manager or coordinator
- Through a phone call to the STEPS Customer Service Officer (CSO) on (07) 5458 3000
- Workers can record verbal complaints on a Tell Us What You Think form (i040102) or by using the *Feedback and Complaint Outlook Form* which can be found in the Organisational Forms Library located here:
    - In Outlook, click on New Items under the Home ribbon
    - In dropdown, click more items and then Choose Form
    - In the Choose Form window when looking in Organisation Forms Library, double-click on Feedback and Complaint and the *Feedback and Complaint Outlook Form* email will open.

Any of the above methods can be used by a customer’s nominated advocate. Complaints can also be made anonymously in line with the National Disability Insurance Scheme (Complaints Management and Resolution) Rules 2018.

In the event of a complaint being posted on social media sites, the Executive Manager - Marketing and Communications will post a response and forward the complaint to STEPS Customer Service Officer (CSO) for processing in accordance with this procedure.

2.3 INFORMING CUSTOMERS

On entry to a service, all customers are to be presented with an information pack relevant to the Service Stream that will include the Feedback and Complaints Policy (i010103) and process.

All customers are to be advised of:

- The processes for raising a complaint
- Details of any external complaint’s resolution bodies
- Their right to access and be supported by an independent advocate of their choice

Reminders of the complaints process should be provided regularly with awareness maintained by the visibility and availability of promotional materials.

2.4 COLLECTION OF COMPLAINTS

Any staff member receiving a complaint, including the STEPS Customer Service Officer (CSO), will forward all complaints to the relevant line manager using the *Feedback and Complaint Outlook Form* located in the Organisational Forms Library in Outlook.

Where a complainant indicates that they do not want to communicate with the direct line manager, the complaint is to be forwarded to the next senior manager using the *Feedback and Complaint Outlook Form* located in the Organisational Forms Library in Outlook.

Refer to section 2.2 Process for Raising Complaints detailing where to find the *Feedback and Complaint Outlook Form.*

2.5 ANTICIPATED RESPONSE TIMES

Action all complaints in a fair, prompt, and confidential manner.

STEPS Customer Service Officer (CSO) or the line manager is required to acknowledge the complaint within the following timeframes listed below:

- Written complaint – as soon as possible (within 24 hours) in writing (email) or using the optional Complaint Acknowledgement Letter (i040104) printed on STEPS letterhead; and
- Verbal complaint – at the time of the complaint

Response times for resolution of complaint should occur within the timeframes specified in section 3.0 Complaints resolution.

2.6 ASSESSMENT OF A COMPLAINT

Some complaints can be resolved quickly through open communication or an apology, however, sometimes the scope of a complaint is not clear, or the complaint is complex, and an investigation may be required to identify the underlying issues.

The line manager will conduct the assessment which will include:

- Clarifying the concerns and issues raised by the complainant
- Determining the level of risk to the wellbeing, safety and health of the client and staff identified in the complaint
- Deciding if priority should be given to one or more aspects of the complaint
- Asking the complainant how they would like to see their complaint resolved.

Resolution can be quite straightforward e.g., an apology, or small change in services. Some complaints are to raise awareness of a problem or ensure that other people do not find themselves in the same situation. The best way to establish a complainant’s expectation is to ask them what they are trying to achieve or what would resolve the complaint for them. If the resolution is inappropriate or disproportionate, it is important to explain why a request cannot be met, and it is equally important to offer an alternative solution, if possible.

To assist in the assessment and resolution of a complaint, the line manager will:

- Define the concerns to be examined
- Identify the resolution the complainant is looking for and whether this expectation can be met
- List the types of information required and the possible sources of the information
- Include complainants, workers, and the care recipient (if this person is not the complainant)
- Provide an estimate of the time it will take to resolve the complaint
- Note any special considerations e.g., sensitive, or confidential information involved

The amount of detail obtained during the assessment should reflect the complexity and seriousness of the issues you are trying to resolve.

2.7 INVESTIGATION OF A COMPLAINT

The purpose of investigation is to gather relevant information that can be used to identify an appropriate solution which will resolve the complaint. Not all complaints require a formal investigation to be resolved. Based on the Assessment of the Complaint, the line manager will determine if an investigation is required, and if so, the most appropriate staff member to conduct the investigation, i.e. the line manager, CSO, executive manager and Managing Director if escalation is required.

Any investigation should be:

Impartial – each complaint must be approached with an open mind and findings should be objective

Confidential – an investigation should be conducted in private. The complainant's confidentiality needs to be respected at all times, and information should only be shared on the 'need to know' basis

Transparent – a complainant should be told about the steps in the complaints process and be given an opportunity to participate in reaching a resolution. Maintain regular contact with all parties to the complaint

Timely – conduct the investigation in a timely manner, keeping in mind the anticipated response times (section 2.5 of this procedure)

Documented – keep written records of any information or finding, keep documentation that is provided by the complainant

Following procedural fairness – complainants should be given an opportunity to comment on information or claims from other sources.

2.8 REGISTERING COMPLAINTS

All complaints, including verbal complaints, are to be recorded in an OSI by STEPS Customer Service Officer (CSO) or relevant line manager within two (2) business days of receipt of the complaint. This includes:

- **Raising an OSI**

  Please note the complaint is not required to be resolved before raising the OSI.

  Each entry in the OSI System is given an OSI number. This acts as the Complaints Register for STEPS.

- **Creating an Electronic Folder**

  The relevant line manager or CSO will create a separate file folder for each complaint in the relevant Complaints folder in 'O' Drive

- **Evidence**

  At a minimum, the following forms of evidence should be collected and saved in the specific complainant's folder on the 'O' Drive

  - All correspondence
  - File notes
  - Interviews with complainant
  - Interviews with staff

2.9 PROCESSING COMPLAINTS

At the time of raising the OSI, the line manager or CSO must indicate if the complaint has been:

- resolved
- requires further action, or
- needs to be escalated.

The Quality Assurance & Risk team will forward the OSI to the appropriate Responsible Person (RP) for resolution or escalate to a senior manager. Where the complaint refers to a manager, the Quality Assurance & Risk team must forward to the next senior line manager.

If a system improvement is required in response to a complaint, a further OSI is to be raised.

Where a service stream has a third-party software system for customer management purposes, e.g. MYP, conversations and actions between the customer and STEPS employee must be recorded with the complaint's OSI number included. If the correspondence is internal, it is to be saved in the relevant Complaints folder in 'O' Drive, not the third-party software.

The Quality Assurance & Risk team will save a copy of the OSI in the electronic complaints folder in 'O' Drive. Complaint OSI's are not published but are able to have reports run for the purposes of the Complaints Register.

3.0 COMPLAINTS RESOLUTION

After the assessment and investigation of the issue(s) raised with the complaint, the line manager will be responsible for initiating a response to the complainant and working with them towards a resolution.

The resolution process can occur in the most appropriate manner for the customer or stakeholder. The optional formal letter template Complaint Outcome Letter (i040105) printed on STEPS letterhead can be used to document:

- the outcome of the complaint and actions taken
- the reasons for the decision, and
- any improvements made and resolution(s).

Copies of all documentation, including file notes of any verbal communication, must be saved into the relevant Complaints folder in 'O' drive.

Resolution of a complaint should occur within:

- 10 business days from when the complaint was made in person, by telephone or via email, or
- 20 business days when the complaint was made in writing.

Where a complaint is not resolved within the above timeframes, the customer or stakeholder must be kept informed and file notes recorded.

3.1 APPEALS

If the complaint is not able to be resolved by the CSO, line manager, or the senior manager, the complaint will be escalated to the Managing Director quickly enough that the resolution of the complaint will still occur within the above timeframes. Customer complaints specifically relating to RTO assessment outcomes should be directed to the Assessment Appeals Procedure (1501800) for resolution.

3.2 EXTERNAL COMPLAINTS RESOLUTION

If the complainant is dissatisfied with the outcome, they may access relevant external agencies to assist in mediation and resolution processes. Interpreter services are available through the Australian Government's Translating and Interpreting Service (TIS National) by calling 131 450. STEPS provide the following information to customers on the applicable external regulatory bodies as required under regulation or contract.

- **National Disability Insurance Scheme (NDIS) Quality and Safeguards**

  Phone: 1800 035 544 (free call from landlines) or TTY 133 677 Interpreters can be arranged.

  Online: Complete a Complaint Contact Form (business.gov.au)

- **Australian Skills Quality Authority (ASQA)**

  Phone: ASQA **Info line** on **1300 701 801** between 9.00 am and 7.00 pm (EST) Monday to Friday or (dial +61 3 8613 3910 from outside Australia).
  Online: Contact ASQA online by completing the Enquiries | Australian Skills Quality Authority (ASQA) form or email enquiries@asqa.gov.au

  Post: ASQA's postal address is GPO Box 9928, Melbourne, VIC 3001

- **Disability Employment Services (DES)**

  Phone: 1800 634 035

  Email: complaints@dss.gov.au

  Post: DSS Feedback, GPO Box 9820, Canberra ACT, 2601

- **Individual Recovery Support Program (IRSP)**
  Sunshine Coast Hospital and Health Service, Patient Liaison Service
  Email: SC-PLO-Inquiry@health.qld.gov.au

  Post: Complete the SCHHS consumer feedback form: compliment, complaint and suggestion for improvement (PDF 108 kB) and send to The Patient Liaison Officer, Patient Safety and Quality Unit, Nambour General Hospital, PO Box 547, Nambour QLD 4560

4.0 REPORTING AND ANALYSIS

Line managers are responsible for ensuring actions taken for resolution are recorded in the OSI System. The Quality Assurance & Risk team is responsible for analysing entries in the OSI System to identify and manage trends, and to recommend system improvements.

The Quality Assurance & Risk team will provide monthly Complaints Reports through the Quality & Compliance Board Report which will be forwarded to:

- the Executive Leadership Team (ELT)
- Board of Directors

Every six (6) months the Quality Assurance & Risk team will:

1. conduct an Internal Audit against the Complaints process
2. analyse complaints to look for commonalities or trends

This analysis can help identify high risk processes and practices to facilitate work on systemic solutions to problems. Trend analysis can also show where the root cause of a problem may lie. This is essential to ensure continual improvement of the services offered by STEPS.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Assessment Appeals Procedure (1501800)	Complaint Acknowledgement Letter (i040104)
Complaint Outcome Letter (i040105)	Complaints Process (i040101)
Feedback and Complaints Policy (i010103)	Feedback Procedure (i040100)
Feedback and Complaint Outlook Form *Refer to Outlook > New Items > More Forms > Choose Form > Organisational Forms Library > Feedback and Complaint*	Incident Management Procedure (i090700)
Tell Us What You Think form (i040102)	WHS Incident Notification Procedure (i090200)

6.0 GOVERNANCE

Document Owner	Manager – Quality Assurance & Risk	**Approval Date**	6 April 2023
Effective Date	11 April 2023	**Document Number**	i040500_v6_230411

(Uncontrolled when printed)

1.12.3 Surveys / Customer Satisfaction

1.0 EVALUATING CUSTOMER SERVICE

STEPS Group of Companies (STEPS) is committed to utilising evidence-based data to deliver high quality services and surveys are used as a marketing research method for evaluating services to our customers

This procedure will ensure that individual surveys are necessary, either to meet strategic objectives or to comply with contractual or legal requirements. Furthermore, the procedure will facilitate in ensuring the data is reliable, valid and will be used to inform decision making.

All surveys must be implemented in accordance with this procedure, excluding general feedback which will be collated and analysed as per the Feedback Procedure (i040100) and Complaints Procedure (i040500).

1.1 DEFINITIONS

Survey	A process of collecting information from persons using various marketing research methods such as electronic or paper questionnaires, focus groups or interviews.
Feedback Collection Methods	A Feedback Collection Method may include electronic or paper questionnaires, focus groups, interviews (face to face, video conference or phone), observation, experiments/field trials, general feedback (social media measurements and analysis can quantify), competitive analysis, public domain data, purchasing of research reports, sales data analysis, and search engine data. A combination of methods could be used depending on requirements.

2.0 SURVEY PRINCIPLES

When preparing a survey request the basic principles of sound survey design should be considered, including:

- A purpose, which is a broad statement of the primary aim or outcome
- Objectives that are specific and measurable steps to meet the survey purpose. The objectives provide a framework for asking the right questions
- Do not consider questions at this stage, start with objectives.
- Methodological design that follows best practice, as appropriate.

3.0 REQUEST FOR APPROVAL TO SURVEY

- Email the Survey Request Form (i040201) to QualityTeam@stepsgroup.com.au at least 30 days prior to the expected survey is to commence.
- Initial approval must be obtained by a member of the Executive Management Team (EMT) and then submitted to the Executive Leadership Team (ELT) for final approval.
- Final approval must be obtained by the Executive Leadership Team (ELT) prior to commencement of survey process.
- Surveys directed by government authorities are exempt from following the survey approval process, however, surveys of this nature must be notified to the Quality Assurance & Risk team via the email QualityTeam@stepsgroup.com.au to be added to any relevant schedules or registers. There is no need to submit a survey request for a survey of this nature.

4.0 SURVEY REQUEST REVIEW

- The Risk and Compliance Manager will review the survey request with the Data Analyst – Quality Systems, and will:
  - Apply timeframes suitable for implementation, considering frequency of other surveys being conducted

- Advise if any similar surveys already implemented may assist with the survey's purpose
- Advise if any other feedback collection methods which may assist with the survey's purpose
- Request further information about expected outcomes of the survey
- Make recommendations to the survey requester to improve the survey quality
- Seek further approvals on behalf of the requester (if required), based on the focus of the survey
- Consider if assistance is required from other departments, in particular the Marketing and Communications Team.

5.0 FINAL OUTCOME OF SURVEY REQUEST

- A final decision to approve or not approve the survey request is made by the Risk and Compliance Manager after discussion with the Data Analyst – Quality Systems. Any conditions in relation to implementation of the survey will also be advised as part of the approval. A notification will be provided via email.
- The approved survey will be added to the survey schedule located in 'O' Drive under the *Surveys* folder located in the Quality Process files.

6.0 TIMEFRAME OR SCOPE CHANGES OF APPROVED SURVEYS

- For any approved surveys, the survey requester must advise the Data Analyst – Quality Systems of any changes to timeframes or target populations as soon as they become aware by emailing QualityTeam@stepsgroup.com.au. This may result in further considerations as per section 4.0.

7.0 SURVEY DESIGN AND COLLECTION METHODS

- Survey design and collection methods will not commence until all requirements have been confirmed and approved by the Risk and Compliance Manager.

8.0 DATA AND FINDINGS

- A summary of findings or a full report will be available depending on survey request and purpose.
- The Risk and Compliance Manager will coordinate a survey findings meeting with the relevant manager/s and Data Analyst – Quality Systems which may result in an action plan and an infographic.
- All survey results and/or findings will be saved in 'O' Drive under the *Surveys'* folder located in the Quality Process files.

- Individual responses are considered private and will be saved in O' Drive under the Quality Management folder.

- Minimum responses for a group is 5 to protect anonymity. If the group is less than 10, the next level grouping will be applied.

9.0 STORAGE AND ACCESS TO INFORMATION

- Survey answers and personal information will be stored in accordance with *Privacy Act 1988 (Cth) (the Privacy Act) and Australian Privacy Principles (APPs).* For more information, refer to Privacy Policy (i010106) which is also available on STEPS website https://www.stepsgroup.com.au/privacy-policy/.

- Shared results from SurveyMonkey will include only aggregated results. Individual responses can only be accessed by the Quality Assurance & Risk Team or relevant Manager on request.

- Sometimes, STEPS may use SurveyMonkey for collection of responses, this means the information is transmitted and stored securely in the United States and is accessed by STEPS in accordance with SurveyMonkey Privacy Policy. You can access SurveyMonkey's terms of use by following this link https://www.surveymonkey.com/mp/legal/terms-of-use/. Respondent will know when SurveyMonkey is used because the footer with SurveyMonkey logo will either be included in the email, or it will be stated. SurveyMonkey is not subject to the *Commonwealth Privacy Act 1988*, and STEPS will not have an obligation to take reasonable steps to ensure that SurveyMonkey does not breach the Australian Privacy Principles in relation to personal information that is given to SurveyMonkey and that you will need to seek redress under the laws of the USA and the EU for any privacy breaches by SurveyMonkey. If an answer is provided, the respondent agrees to the transmission of their information as described above. If a respondent declines to give their answer, STEPS will endeavour to provide a different contact or method to complete their response to the survey.

10.0 RELATED DOCUMENTS

Document Name	Document Name
Complaints Procedure (i040500)	Feedback Procedure (i040100)
Privacy Policy (i010106)	Survey Request Form (i040201)
Survey Schedule located in the O drive	

11.0 GOVERNANCE

Document Owner	Risk and Compliance Manager	**Approval Date**	23 May 2024
Effective Date	27 May 2024	**Document Number**	i040200_v3_240527

(Uncontrolled when printed)

1.13 Financial Management, Assets and Vehicles

The Finance department is the central hub for the organisation's finance activities which incorporate all of the following:

- All debtor and creditor invoices and payments;
- Expense claims;
- Cash floats;
- Program income and expenditure tracking to ensure compliance with government contracts and acquittals submitted where required;
- Site income and expenditure monitored to ensure viability of each site;
- Centralised budgeting done annually and re-forecasts done as necessary;
- Adhoc tenders and changes to contracts evaluated;
- Monthly Profit and Loss and Balance sheets generated for Board approval;
- Annual financial audit; and
- Asset management.

Frequently used forms are listed below, for all other related Procedures & Documents refer to the Financial Management, Assets and Vehicles Chapter link

Entry Notice Form (e310001)

Office Share Agreement Instructions (e310005)

Property Inspection Form (e310006)

1.13.1 Corporate Credit Cards

CORPORATE CREDIT CARDS

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has adopted the ANZ Visa Card to assist the purchase of goods and services on behalf of the organisation. The benefits of the card include the reduction of administration costs and paperwork in purchases of lower value. Where a corporate credit card is not available for minor purchases at sites, other avenues of payment options can be explored with the

Finance team such as the establishment of local corporate accounts, and / or reimbursement through the staff reimbursement process.

The purpose of this procedure is to establish clear and definite requirements about how credit cards issued to employees are utilised. This is to ensure all credit card expenditure is appropriately authorised and is for an approved purpose. Clear guidance about the use of corporate credit cards is to ensure employees issued with corporate credit cards understand their responsibilities and obligations.

2.0 FINANCE DEPARTMENT RESPONSIBILITIES

The Chief Financial Officer (CFO) is responsible for the operation and control of the credit card system and has authority to immediately cancel any card considered as being misused. The CFO may also set and vary the credit limit of any card.

The CFO is responsible for establishing card accounts and the issuance and cancellation of cards.

Requests for new cards (or variations to existing cards) are to be forwarded, via the appropriate manager, to the CFO. Credit cards will be issued where a role requires the use of a credit card, and transaction limits will be determined in line with the delegations register.

3.0 EMPLOYEE RESPONSIBILITIES

The cardholder will acknowledge that they are aware of the responsibilities and restrictions placed on their use of the card prior to taking possession of the card.

The user has the authority to incur expenditure up to the limits (individual transaction limit and overall card limit) on their card for approved STEPS purchases. Splitting of purchases to avoid card limits is not permitted. Where card limits are preventing a required purchase, the user must contact the Finance department to discuss alternate payment options.

The user is responsible for the security of the card and must understand they are personally accountable for the expenditure on their card.

Cardholders must not allow another person to use their Corporate Credit Card. Exceptions to this is where Executive Assistants may be required to make bookings on behalf of the cardholder; and within the HR team for the purchase of criminal history checks.

When the cardholder is on leave, the card is not be given to another staff member to use in the cardholder’s absence. Where this is longer planned leave, such as long service leave, the Finance department can temporarily reduce the card limit to Nil for the leave period.

Evidence of each transaction and authority to incur the expenditure must be retained.

A tax invoice or receipt is required for every transaction. In the absence of a tax invoice or receipt a Statutory Declaration must be completed, except for parking expenses where receipts are not issued.

Cardholders are to notify the Finance department of any disputed credit card transactions. The Finance department will provide guidance as to appropriate actions.

If a card holder resigns or separates from the organisation, the cardholder must return the card and all supporting coded documentation to their supervisor/manager for cancellation.

4.0 PROCESSING CREDIT CARD STATEMENTS

Throughout the credit card statement period when money is spent on the credit card the expense line is automatically created within the Expense Management System (ProSpend). The cardholder is able to attach receipts and appropriately code these expenses throughout the month.

At the end of the credit card statement period the credit card claim status will change to ‘Ready’ and the cardholder will be sent an email advising that the visa claim is ready to submit. The visa claim must be submitted for approval within two weeks of the claim being marked as ‘Ready’.

Prior to submission, a Department Code, Program Code, Expense type and a description must be assigned to each expense transaction.

Upon submission, the credit card claim will be submitted to the cardholders’ line manager for approval. Once the credit card claim has been approved and is marked as finalised in the Expense Management System, the physical tax invoice or receipt can be discarded.

When using the credit card for the first time, the cardholder should watch the ProSpend Training Video on the STEPS Information Destination (SID) and contact the Finance Department to arrange additional training if required.

5.0 APPROPRIATE USE

The card may only be used for authorised official STEPS purposes for an amount determined by your manager. (The Delegations Register will give you the maximum value for the dollar limit of a purchase).

The user must not exceed the monthly credit limit.

The card may be used for telephone/internet purchases.

On receipt of the goods or services the user should obtain a Tax invoice or Receipt from the supplier.

6.0 INAPPROPRIATE USE

The card is NOT to be used in ATM machines to obtain cash advances.

The card is NOT to be used to purchase goods for personal use which are not related to work. If the card has been used for personal use in error, this amount must be repaid to STEPS immediately.

The card is NOT to be used where we have a corporate account or where we are able to pay on invoice by EFT.

The card is NOT to be used for purchase of gift cards for customers, participants and students. Purchases of gift cards is managed as per the purchasing gift cards procedure.

Misuse of issued cards may necessitate STEPS to undertake formal disciplinary and/or legal action against the cardholder.

7.0 LOST OR STOLEN CARDS

If at any stage a card is lost, stolen, or fraudulent activity is noticed on the card, the employee must notify the Finance department and ANZ immediately. It should be noted that until the bank is notified all costs incurred on the card are the responsibility of the organisation.

8.0 DECLARATION

Employees must sign this page, retain a copy for their records and return original to Finance.

I, ____ (employee name) have read, understood and agree to comply with the Corporate Credit Cards Procedure with Employee Declaration (e310400).

Employee Name			
Employee Signature		**Date**	

9. RELATED DOCUMENTS

Document Name	Document Name
Delegations Register (i010601)	Gift Card Procedure (Awaiting Approval)

10. GOVERNANCE

Document Owner	Chief Financial Officer	**Approval Date**	24 June 2024
Effective Date	5 July 2024	**Document Number**	e310400_v4_240705

(Uncontrolled when printed)

To access a print friendly version of this procedure please click here.

1.13.2 Driving Company Motor Vehicles with Employee Declaration

1.0 COMPANY VEHICLES

STEPS Group of Companies (STEPS) provides vehicles for use by managers, employees and selected volunteers who are required to attend to work related matters including visiting, supporting and transporting clients to relevant community activities.

1.1 RESPONSIBILITIES

Executive Leadership Team (ELT) will:

- Ensure that sufficient resources are allocated to fully implement this procedure.

Supervisors will:

- Ensure that all requirements for provision of vehicles are appropriately assessed, are maintained and employees and selected volunteers are appropriately licensed and competent to use the vehicles.

- Ensure that personnel comply with all requirements for safe use of company vehicles.

Employees will:

- Ensure any vehicle driven is properly cared for and maintained; traffic incidents are reported immediately.
- Ensure all vehicles are driven safely and in compliance with this procedure.

1.2 EVIDENCE OF CURRENT LICENCE

All employees must upload a copy of their driver's licence to ConnX. It is the employee's responsibility to ensure that the licence is kept current. The Human Resources Information System (HRIS) sends a reminder email to the employee and their manager 60 days prior to their licence expiring. Human Resources (HR) conduct monthly checks to ensure all licences are current.

Selected Volunteers who are given authority to drive a company vehicle must give a copy of their driver's licence to the nominated Volunteer Coordinator for records. It is the volunteer's responsibility to ensure that the licence is kept current.

Both employees and volunteers must report changes to driver privileges, such as driver's licence suspension, immediately.

Employees on their Red P Licence are not permitted to drive STEPS vehicles, nor are they permitted to have clients in their own vehicle.

1.3 JOURNEY PLANNING

All employees and selected volunteers are reminded of driver fatigue and the dangers involved when driving a vehicle whilst tired. Any person required to travel to remote locations must complete the Fatigue Management and Isolated Work or Working Alone Checklist (i050601).

Prior to travelling all employees should consider the following:

- Plan adequate rest breaks when driving long distances
- Communications regarding departure and confirmation of arrival
- Risk of travelling before dawn and after dusk
- Awareness of wildlife when driving
- Workers should avoid travelling at night on company business; if unavoidable, only when necessary and be kept to a minimum
- Speed limits must be adhered to
- If employees and selected volunteers have been working in the sun all day, ensure that they have had appropriate sun cover and are rehydrated for the journey home.

1.4 PRE-OPERATIONAL SAFETY CHECKS

- Employees must book the vehicle through the booking system
- Employees must ensure that the vehicle is checked out in the booking system at the time they collect the keys
- Employees must locate and ensure familiarity with all vehicle operations and controls
- Complete a vehicle prestart prior to commencing any work-related travel and identify any damage or maintenance that is required. Employees are to complete the vehicle prestart via the Fleet Office App which is to be loaded onto their work device or personal mobile phone
- Report any problems to the Supervisor

- Take time to set up the vehicle before driving, alter seat and mirrors to suit you physically
- Check fuel levels
- Plan your route to ensure your concentration on driving not navigating
- Know the Traffic Regulations.

1.5 DRIVING VEHICLES

- Driver’s licences must be valid
- Seatbelts must be worn at all times
- Using a mobile phone when driving is prohibited for learner drivers, P plater or probationary licence holders under the age of 25 years. All other licensed drivers must be connected to blue tooth and hands free
- No smoking in vehicles at any time
- No animals are allowed in vehicles at any time with the exception of assistance animals
- STEPS reserves the right to fit any tracking system including GPS enabled tracking
- All speed limits must be adhered to
- Each vehicle has a fuel card which is located in the glove box or centre console of the vehicle to purchase approved petrol and oil for STEPS related activities only. No miscellaneous purchases are permitted on these cards
- Always be alert to any changes in performance, gauges or noises react accordingly, pull over and check, fix if possible, get the problem fixed by a professional or report to Supervisor
- Be aware of the vehicles capabilities in choosing the type of roads, the weather and the speed you travel considering conditions
- Avoid road rage and accidents by being considerate and alert while driving
- Avoid fatigue resting every 2 hours as a minimum, not driving if fatigued from previous night

1.6 OBLIGATIONS

- The vehicle is to be serviced as per the set manufacturers guidelines (the servicing fees are arranged and paid by STEPS through our Fleet Company however it is the responsibility of the driver to ensure they have booked for servicing, repairs as per the manufacturers guidelines)
- The driver is responsible for any parking tickets, driving offence tickets associated with the car
- The driver must advise STEPS of any parking tickets, driving offence tickets or charges immediately
- The driver is to refer to the Fitness for Work Policy (i010104) and the Drugs and Alcohol in the Workplace Procedure (i051100) to further understand their obligations and STEPS expectations as an employee of STEPS. An employee who is found to have driven under the influence of alcohol or drugs may be dismissed
- The driver must drive and handle the car responsibly and follow all State and Federal Road Rules to the letter of the law
- In the instance of a breakdown refer to the Motor Vehicle Breakdown / Accident Information (i050302) sheet located in the glove-box

- Vehicles are not permitted for private use unless approved by the Managing Director. When regular private usage is permitted, a letter of agreement or terms and conditions of the employees' contract of employment will detail the extent of private usage allowed
- The driver must complete the WHS Incident Report (i090201) immediately following any incident
- In the event of a traffic incident:
    - Ensure that you and all occupants are safe, well and out of traffic lanes to prevent further incidents and injury
    - Refer to the Motor Vehicle Breakdown / Accident Information (i050302) sheet located in the glove-box
    - Call your manager immediately and complete the Motor Vehicle Accident Claim (i050301) within 24 hours. Your manager will then advise whether a WHS Incident Report (i090201) is required to be completed. Forward a copy of the completed paperwork to your manager and the finance department
    - Call 000 for assistance from emergency services if required
    - Attend to or assist with first aid – if you are a trained and competent first aider
    - Where the driver of a STEPS company vehicle is at fault and charged with 'Driving Under the Influence', is not licensed to drive, uses or allows the company vehicle to be used in a manner that voids insurance or is negligent, STEPS may choose to take legal action against the driver to recover costs of repairing / replacing the vehicle
    - STEPS will only pay the excess for one insurance claim within each completed year of service (not cumulative) where an employee is deemed to be 'at fault' by the insurer. The employee will be required to pay excess for any further claims where they are deemed to be 'at fault' by the insurer within that year of service
    - **DO NOT MAKE STATEMENT OF GUILT** – regardless of the cause of the incident.
- **ENSURE THAT YOU OBTAIN THE FOLLOWING DETAILS FROM OTHER DRIVER/S AT THE SCENE:**
    - Vehicle make and colour
    - Registration number
    - Name, address, and contact details of driver
    - Licence number of the driver or take a photo of their licence (both sides)
    - Name of their insurance company (and policy number if possible)
    - Take photos (phone camera) of the damage to the other vehicle/s
    - Take photos of damage to the STEPS or your vehicle.

      Also note:
        - the date and time of the accident; and
        - names and contact details for any witnesses.

1.7 ENDING OPERATIONS AND CLEANING UP

- Report anything out of the ordinary to the Supervisor on return to office or completion of shift
- Leave the vehicle in a safe, clean, tidy state with at least a 1/4 tank of fuel and tyre pressure is adequate

- Ensure that the vehicle is checked in on the booking system and keys are returned to the appropriate location.

1.8 HOME GARAGING

- Where there is an operational need for a general fleet vehicle to be garaged off site at the home of a staff member, the vehicle may be assigned to a designated driver with the prior approval of the Managing Director
- A vehicle provided for home garaging can only be driven outside of work hours by the staff member to drive to and from work. There are no other personal usage rights provided except where approved by the Managing Director
- Personal use includes using the vehicle for personal errands between business activities, to commute between the workplace and home, or using the vehicle outside of business hours
- The staff member must park the vehicle in a secure and protected place at their usual place of residence and must ensure the vehicle is kept locked when not in use.

2.0 DECLARATION

(Please print the Driving Company Motor Vehicles Procedure with Employee Declaration (i050300) for employees and volunteers to read and sign).

Employees must sign this page, retain a copy for their records and upload a signed copy to ConnX. Volunteers must sign this page, retain a copy for their records and return the original to the Volunteer Coordinator.

I,______________________________________, (employee/volunteer name) have read, understood and agree to comply with the Driving Company Motor Vehicles Procedure with Employee Declaration (i050300).

Employee Name			
Employee Signature		**Date**	

3.0 RELATED DOCUMENTS

Document Name	Document Name
Drugs and Alcohol in the Workplace Procedure (i051100)	Fatigue Management and Isolated Work or Working Alone Checklist (i050601)
Fitness for Work Policy (i010104)	Motor Vehicle Accident Claim (i050301)
Motor Vehicle Breakdown / Accident Information (i050302)	WHS Incident Report (i090201)

4.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	6 April 2023
Effective Date	18 April 2023	**Document Number**	i050300_v11_230418

(Uncontrolled when printed)

To access a print friendly version of this procedure please click here

1.13.3 Financial Management

1.0 FINANCIAL MANAGEMENT

STEPS Group of Companies (STEPS) is committed to the effective and efficient use of program funds. Ensuring programs are delivered in a cost effective manner whilst maintaining a high quality of service delivery.

1.1 RESPONSIBILITIES

Chief Financial Officer (CFO)

The Chief Financial Officer (CFO) is responsible for the development of annual budgets. The Board, Managing Director (MD)/Chief Executive Officer (CEO) and Executive Leadership Team (ELT) will be included in this process.

The CFO is responsible for the maintenance of financial records and generating of financial reports. The CFO is responsible for the annual financial audit.

2.0 BUDGETS

The annual budget planning process will commence with enough time so that a budget will be ready for Board approval by the end of June.

During the first week of the third month of each quarter, the CFO and MD/CEO will decide if a quarterly re-forecasting process will be done. Where there has been substantial change within STEPS, a re-forecast will be done.

A re-forecast should be completed within 15 working days of the end of the quarter otherwise its value diminishes.

3.0 REPORTS

Financial Reports that will be produced on a monthly basis for the group and all its entities where applicable will include:

- Balance Sheet

- Statement of Profit or Loss, and where applicable with variance to budget
- Aged Creditors Report
- Aged Debtors Report
- Ad hoc reports where required

In addition to the above, financial reports that will be produced on a yearly basis and may include:

- Cash Flow Statement
- Assets Register

The financial reports will be produced in a summary form for the Board and in detail for the Audit Committee and Management.

4.0 AUDITS

All entities will be audited by an independent and accredited auditor on an annual basis but no later than the 31 August of each financial year.

The Board will approve the appointment of the auditor each year at the Annual General Meeting.

An audit file for each entity is to be prepared for the auditor by the Finance Manager.

5.0 RELATED DOCUMENTS

Document Name
Nil

6.0 GOVERNANCE

Document Owner	Chief Financial Officer	**Approval Date**	19 July 2023
Effective Date	8 August 2023	**Document Number**	e310200_v2_230808

(Uncontrolled when printed)

1.13.4 Fraud Control

1.0 PURPOSE

This procedure establishes the organisational procedures for controlling the risk of fraud. Our approach is underpinned by principles of sound risk management and strong quality management systems which are developed, reviewed and continually improved to provide a robust framework for consistent application of processes that support high levels of compliance with regulatory and contractual requirements.

This procedure applies to all employees across STEPS Group of Companies (STEPS) and its related entities and brands.

Within the scope of this procedure, fraudulent conduct includes:

- Theft of inventory and equipment by employees.
- False invoicing and accounting.
- Theft of funds.
- Use of misleading or inaccurate information for the purposes of deceiving, misleading or to hide wrongdoing.
- False or misleading information in the course of employment, or absence from duty without leave or good cause.
- Incorrect claiming of funds from the Commonwealth.

1.1. DEFINITIONS

Fraud	Involves the use of dishonest or deceitful conduct in order to obtain a benefit or advantage.

2.0 PROCEDURE

It is accepted that fraud presents an enterprise risk in terms of financial loss, reputational impact, diversion of management energy and organisational morale. To mitigate against such risks, STEPS operates under the governance principles of full disclosure of all financial transactions, policies and an organisational-wide commitment to acting ethically and with integrity.

All employees are provided with a copy of the STEPS Code of Conduct and Ethical Behaviour (e210007) and demonstrate their commitment to this by signing on appointment.

Accountability for fraud planning rests with the Managing Director (MD) and the Senior Managers of each Service Stream within STEPS.

Fraud risk assessment will be undertaken by the MD and the Executive Leadership Team (ELT) in accordance with the Risk Management Procedure (i050100).

Risk mitigation and control systems will include restricted and secure access to electronic systems, regular monitoring of financial transaction records, quality control of suppliers (refer Procurement Procedure [i030100]), staff education and training, internal audits (refer Audits Procedure [i060300]), commitment to the STEPS Code of Conduct and Ethical Behaviour (e210007) and pre-employment screening of all new employees (refer Criminal History Check Procedure [e200200]).

STEPS endeavours to ensure that all funds claimed from the Commonwealth and/or State are made in accordance with the relevant contract/s and guidelines (where available) which are supported by information on the STEPS Quality Manual (SQM) and through the risk mitigation measure identified in the Risk Management Procedure (i050100).

Suspicion or knowledge of illegal or unethical conduct should be reported to the appropriate line manager or the MD, who is responsible for bringing the matter to the attention of the Executive Leadership Team and/or the Board of Management.

Reports may be made anonymously and directly to the MD/ELT. Preliminary investigations will be undertaken to confirm the veracity of anonymous information prior to the instigation of a full investigation, which will only proceed based on supporting evidence.

Investigation of suspected fraudulent conduct will be undertaken by a nominated representative of the ELT or Board of Management, alternatively a contracted third party may be appointed. All external parties will be required to enter into a binding agreement of confidentiality to ensure the information coming into possession during the course of the investigation remain confidential.

Where there is clear evidence of fraud, recovery action may be undertaken.

Fraud is considered an act of serious misconduct and may constitute grounds for immediate termination.

3.0 RELATED DOCUMENTS

Document Name	Document Name
Audits Procedure (i060300)	Criminal History Check Procedure (e200200)
Procurement Procedure (i030100)	Risk Management Procedure (i050100)
STEPS Code of Conduct and Ethical Behaviour (e210007)	

4.0 GOVERNANCE

Document Owner	Chief Financial Officer	**Approval Date**	25 July 2024
Effective Date	30 July 2024	**Document Number**	i030300_v3_240730

(Uncontrolled when printed)

1.13.5 Fraud and Corruption Prevention and Control

FRAUD AND CORRUPTION PREVENTION AND CONTROL

1.0 INTRODUCTION / GENERAL

STEPS Group of Companies (STEPS) is committed to the prevention, deterrence, detection and investigation of all forms of fraud. STEPS aims to control fraud and corruption within its operations as fraud inevitably leads to loss that can be either financial or reputational.

Every employee and volunteer has a responsibility to assist STEPS to prevent, detect and report fraud and corruption. STEPS relies on each person within the organisation to assist in the prevention, detection and reporting of fraud and corruption because we are in an environment experiencing rapid change, with an increasing use of technology, a greater diversity in services and we are geographically dispersed.

To assist employees and volunteers STEPS will maintain internal procedures to prevent and/or detect any fraudulent activity. Included in this procedure is the provision for ‘Confidential Reporting and Protection’ which supports the principles of the AS 8004-2003 Whistleblower Protection Program for Entities.

This Procedure should be read in conjunction with the Fraud and Corruption Prevention and Control Policy (i010108); Fraud Control (i030300); Conflict of Interest Procedure (i010500); Code of Conduct and Ethical Behaviour (e210007), Whistleblower Procedure (i090500) and Accepting Gifts and Benefits Procedure (i010800). These documents outline STEPS’ commitment to fraud and corruption prevention and how this is to be implemented, managed and reported.

STEPS Fraud and Corruption Prevention and Control Policy (i010108) and Fraud and Corruption Prevention and Control Procedure (i030400); documentation is based on the guidelines and principles of AS 8001-2008 Fraud and Corruption Control.

1.1 DEFINITIONS

Fraud	Dishonest activity causing actual or potential financial loss to any person or entity and also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit. (as per the AS 8001-2008).
Corruption	Dishonest activity in which a director, executive, manager, employee or contractor of an entity acts contrary to the interests of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or entity. The concept of ‘corruption’ can also involve corrupt conduct by the entity, or a person purporting to act on behalf of and in the interests of the entity, in order to secure some form of improper advantage for the entity either directly or indirectly. (as per AS 8001-2008).
Confidential Reporting and Protection	This is an important element of the detection of fraud and corruption to encourage the reporting of ‘reportable conduct’. Reports will be handled in a way that protects the person reporting whilst enabling investigation of the allegations to occur by the Fraud and Corruption Control Office.
False Reporting	False reporting where it is shown that a person has made a false report of reportable conduct, then that conduct itself will be considered serious and may result in disciplinary proceedings in accordance with the relevant procedures.
Reportable Conduct	Includes the following actions, which are considered to fall within the definition of fraud and corruption (the list is not exhaustive): • theft of company property, including information; • use or sale of company assets for personal gain; • forgery or alteration of company documents; [for example Inflated and/or faked expense claims or timesheets] • wilful destruction or removal of company records;

	• making or using forged or falsified documents or signatures; • payments to phantom employees/ suppliers or payment to an employee for tasks not performed; • false claims for entitlements or benefit e.g. false information on timesheets; • unauthorised disclosure of confidential information to outside parties; • running private business in work hours; • undertaking or assisting in illegal activity; • acceptance of bribes or gifts to favour third parties; • negligent or deliberate mis-management of contracts; • knowingly generating or paying false claims or invoices; • incorrect claiming of funds from the Commonwealth. • use or disclosure of personal information for an improper purpose; • unauthorised or unlawful alternation of personal information; • unlawful alteration, destruction, forgery or manipulation of data for fraudulent purposes; • providing false or misleading information; • failing to disclose a conflict of interest; • failing to provide information where there is a legal obligation to do so.

2.0 RESPONSIBILITIES

Responsibility for fraud and corrupt conduct prevention rests with all STEPS employees and volunteers, contractors, participants and service users. All parties must comply with the Fraud and Corruption Prevention and Control Policy (i010108) and the Fraud and Corruption Prevention and Control Procedure (i030400);

2.1 EMPLOYEES AND VOLUNTEERS RESPONSIBILITIES

Employees and Volunteers are responsible for

- immediately reporting known or suspected fraud, or instances of unethical or illegal behaviour within the company. The procedure to follow when reporting suspected fraud is as set out in Section 4.1
- reporting perceived weaknesses in internal control to their direct line manager/supervisor;
- assisting in any fraud Investigation;

- maintaining confidentiality and privacy in relation to fraud, or suspected fraud investigation to ensure it does not compromise the investigation or adversely impact on any innocent party.

2.2 MANAGING DIRECTOR RESPONSIBILITIES

The Managing Director (MD) is responsible for:

- ensuring that appropriate and effective internal controls systems are in place that will assist in preventing and detecting fraud and corruption;
- referring to, or notifying, relevant external agencies of allegations of suspected fraud or corrupt conduct in accordance with legislative requirements;
- authorising all alleged fraud and corruption investigations; and
- advising the Board of any fraudulent or corrupt activity or event.

2.3 ELT AND EMT RESPONSIBILITIES

Executive Leadership Team (ELT) and Executive Management Team (EMT) are responsible for:

- endorsement and support for the STEPS Fraud and Corruption Prevention Framework 3.1;
- maintaining the highest standard of ethical behaviour;
- identifying areas of fraud and corruption exposure within their area of responsibility;
- implementing controls to eliminate or reduce fraud or corruption within their area of responsibility;
- ensuring all employees and volunteers receive information on fraud and corruption during their induction
- giving guidance or instructions to staff members on fraud and corruption reporting;
- ensuring contractors are made aware of STEPS Fraud and Corruption Prevention and Control Policy (i010108) and their responsibilities as Contractors;
- make contractors aware of STEPS's Fraud and Corruption Prevention and Control Policy (i010108) and ensure their work is carried out in accordance with their contractual obligations;
- developing and establishing preventative and detective fraud controls and procedures within their area of responsibility;
- carrying out fraud and corruption risk assessments on key functions or areas of exposure within their area of responsibility.

2.4 MANAGERS/SUPERVISORS RESPONSIBILITIES

Managers/Supervisors are responsible for:

- assisting in identifying and then implementing fraud and corruption control measures for programs delivered by employees reporting to them;
- ensuring all employees and volunteers receive information on fraud and corruption during their induction

- giving guidance or instructions to staff members on fraud and corruption reporting;
- make contractors are made aware of STEPS's Fraud and Corruption Prevention and Control Policy (i010108) and ensure their work is carried out in accordance with their contractual obligations;
- Undertake performance management activities and disciplinary matters through the application of reasonable management action and the Disciplinary Action and Effective Termination Procedure (e210600) and Managing under Performance (e220300), seeking support and escalating to relevant ELT/SLT member and HR.

3.0 PREVENTION

STEPS will aim to ensure that it maintains a sustainable ethical culture that aligns with its value of 'integrity'. In addition, STEPS will establish and maintain a strong internal control system where key internal controls are documented and regular reviews are undertaken.

Senior management will demonstrate a high level of commitment to maintaining an ethical culture through observable adherence to STEPS' values and by actively promoting such a culture and ensuring that all employees and volunteers know that behaviours need to be consistent with the Code of Conduct and Ethical Behaviour (e210007) at all times.

All STEPS Workers should have a general awareness of fraud and corruption and how they should respond if this type of activity is detected or suspected.

3.1 THE FRAUD AND CORRUPTION PREVENTION FRAMEWORK

The Fraud and Corruption Prevention Framework at STEPS consists of:

a) Integrated policy including

  - Code of Conduct and Ethical Behaviour (e210007);
  - Procurement Procedure (i030100);
  - Fraud and Corruption Prevention and Control Policy (i010108);
  - Fraud and Corruption Prevention and Control Procedure (i030400);
  - Fraud Control (i030300);
  - Conflict of Interest Procedure (i010500);
  - Accepting Gifts and Benefits Procedure (i010800);
  - Whistleblower Procedure (i090500)

b) Risk assessment and management as per Risk Management Procedure (i050100);

c) Internal controls documented within business processes;

  - Audit Committee
  - Internal reporting;

- External reporting;
- Investigation management;
- Training and awareness
- Internal and External audit process as per Audits Procedure (i060300)

4.0 DETECTION

STEPS will implement risk assessments and systems aimed at identifying instances of fraud and corruption in the event that prevention strategies fail.

STEPS uses proactive fraud detection procedures such as: data analysis, continuous auditing techniques, and other technology tools to detect fraudulent and corrupt activities. These risk mitigation and control systems are described in detail in the Fraud Control (i030300).

STEPS endeavours to ensure that all funds claimed from the Commonwealth and/or State are made in accordance with the relevant contract/s and guidelines (where available) which are supported by information on the STEPS Quality Manual (SQM) and through the risk mitigation measure identified in Risk Management (i050100).

4.1 REPORTING FRAUDULENT OR CORRUPT ACTIVITY

Reporting plays a crucial role in controlling and detecting fraud and corruption.

Any instance of a suspected or actual fraudulent or corrupt event must be reported immediately to the direct manager/ supervisor. The initial report to the direct manager/supervisor can be verbal. The direct manager/supervisor will be responsible for documenting the information and advising the ELT of the allegation.

If an employee or volunteer is unable to report the matter to their direct manager/ supervisor, or if they are absent, the report can be made to the next senior manager/ supervisor (i.e. the manager once removed) Alternatively, the report can be made directly to the ELT or EMT which includes directly to the MD..

Confidential reporting of any suspected fraudulent or corrupt event or activity can be reported to the MD or a member of the ELT or EMT (for more information on confidential reporting refer to the Whistleblower Procedure (i090500).

When making a report, as much detailed information as possible should be provided so that a full and proper investigation can be made. The information should include:

- Name of suspected person/persons;
- Type of fraudulent or corrupt activity that has occurred;
- Date/s that the suspected fraudulent or corrupt activity has occurred;
- Location where the suspected fraudulent or corrupt activity has occurred; and
- Any other relevant information e.g. evidence that you may have concerning the suspected fraud.

All allegations will be reported to the Board.

5.0 RESPONSE

In the event that fraud or corruption is detected or suspected, the MD may choose from any, or all of the following:

- referring to, or notifying, relevant external agencies of allegations of suspected fraud or corrupt conduct in accordance with legislative requirements;
- authorising all alleged fraud and corruption investigations; and
- advising the Board of any fraudulent or corrupt activity or event,
- advise the appropriate government body or law enforcement agency as per Section 5.1.

In the case of suspected corrupt conduct not requiring external body notification, or in circumstances where such external body has referred the matter back to STEPS, STEPS will adopt a comprehensive approach to the subsequent investigation, disciplinary proceedings, prosecution or recovery action.

5.1 EXTERNAL REPORTING

STEPS will have a mechanism in place for assessing fraud and corruption matters and determining its obligations for reporting them to relevant external agencies.

External agencies to which reports on fraud and corruption are made will be determined by contractual requirements and legislation and may include such agencies as the Relevant State Police Service.

The MD will be responsible for determining any referral of fraud and corruption allegations or associated matters to the appropriate external agencies.

5.2 INVESTIGATION

Preliminary investigations will be undertaken with the objective of locating evidence that either substantiates or refutes the claims made (including confidential reports) prior to the instigation of a full investigation, which will only proceed based on supporting evidence.

Investigation of suspected fraudulent conduct will be undertaken by a nominated representative of the ELT or Board of Management, alternatively a contracted third party may be appointed.

All external parties will be required to enter into a binding agreement of confidentiality to ensure the information coming into possession during the course of the investigation remain confidential.

The principles of natural justice will apply. These include:

- A person is presumed innocent until proven guilty.
- A person suspected of fraud has the right to respond to the allegations made and also has the right to be represented at any formal disciplinary proceedings

5.3 FRAUD AND CORRUPTION REGISTER

The Chief Financial Officer (CFO) will maintain a Fraud and Corruption incident register.

5.4 DISCIPLINARY PROCEDURES

Fraud is considered an act of serious misconduct and may constitute grounds for immediate termination.

In some circumstances, an incident may technically meet the definition of fraud, but the evidence may not be able to establish the intention or conduct required to satisfy serious misconduct. In these situations, it is important that the information, response and reasons for action taken are recorded. Any response needs to be proportionate to the level on non-compliance or misconduct. The Executive Manager – Human Resources can assist in developing an appropriate response.

All records in relation to any disciplinary outcomes will be stored on the employees file, according to the Disciplinary Action and Effective Termination Procedure (e210600) and Managing under Performance (e220300).

5.5 RECOVERY OF LOSSES

Where there is clear evidence of fraud, recovery action may be undertaken.

5.6 INTERNAL CONTROLS

In each instance where fraud is detected the Executive Manager/s who have responsibility for the program/s, in conjunction with the Chief Administrative Officer and the Manager - Quality Assurance & Risk will be responsible for assessing the adequacy of internal controls and consider whether improvements are required.

The internal control environment will be reviewed by the Fraud and Corruption Officer every two years at a minimum. This review sill occur in addition to any internal or external audits conducted.

6.0 TRAINING AND AWARENESS

All employees and volunteers will be made aware of the STEPS approach on fraud and corruption, how to recognise corrupt practices, the mechanisms available for reporting corrupt activity during their induction

All employees are provided with a copy of the STEPS Code of Conduct and Ethical Behaviour (e210007) and demonstrate their commitment to this by signing on appointment.

7.0 RELATED DOCUMENTS

Document Name	Document Name
Accepting Gifts and Benefits (i010800)	Audits (i060300)
Code of Conduct and Ethical Behaviour (e210007)	Conflict of Interest (i010500)
Disciplinary Action and Effective Termination Procedure (e210600)	Fraud and Corruption Prevention and Control Policy (i010108)

Fraud and Corruption Prevention and Control Procedure (i030400)	Fraud Control (i030300)
Fraud Control Plan – Disability Employment Services (DES) (i030401)	Managing under Performance (e220300)
Procurement (i030100)	Risk Management (i050100)
Whistleblower Procedure (i090500)	

8.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	5 October 2021
Effective Date	12 October 2021	**Document Number**	i030400_v2_211012

(Uncontrolled when printed)

1.13.6 Insurance

1.0 INTRODUCTION

To ensure all insurance requirements are established, renewed and updated annually to provide adequate cover, and where applicable, meet contractual requirements. Ensure all insurance claims are processed and lodged efficiently and accurately through relevant insurance providers.

1.1 RESPONSIBILITIES

The Managing Director (MD) has ultimate responsibility for ensuring this procedure is adhered too. The Asset Manager (AM) is responsible for the day-to-day operations.

2.0 ESTABLISHING NEW INSURANCE POLICIES

When required, the AM will obtain quotes from preferred suppliers for insurance cover if not provided with existing policies. AM to record details of new policy in relevant file. CFO to update the Insurance Policy Schedule Register located in the Insurance files on ‘O’ Drive. AM to raise an OSI to have the new Certificates of Currency uploaded to the STEPS Quality Manual (SQM).

3.0 RENEWING INSURANCE POLICIES AND COVERAGE

Asset Manager to:

- obtain new quotes each year.
- ensure all insurance policies are renewed and updated annually.
- ensure upon renewing all insurance policies, a review is undertaken to ensure adequate cover, and if required, at a minimum meets contractual requirements.

- record details of policy within relevant file.
- raise an OSI to have the Certificates of Currency for the renewed insurance policies updated on the SQM.

CFO to update the Insurance Policy Schedule Register located in the Finance files on 'O' Drive.

STEPS Group Australia (STEPS) holds various types of insurance.

4.0 WORKERS COMPENSATION INSURANCE

Actual and estimated wages to be declared annually. Actual figures are to be obtained from Finance. The estimated figures will be obtained from the previous 12 months actuals and any anticipated variation. Utilising Human Resources (HR) data, ensure that we have relevant cover in each state or territory. Actual and estimated wages will be declared for each relevant state or territory within the desired timeframes.

5.0 LODGING AN INSURANCE CLAIM

Employees are to notify the AM of any incident / loss and / or damage at their earliest convenience. Employees are to provide detailed information of the incident / loss and / or damage to the AM for the processing of the claim. Employees Manager to ensure (if relevant) employee has completed the Motor Vehicle Accident Claim (i050301) if insurance claim is in pursuant to a motor vehicle claim.

Asset Manager to:

- lodge claim through the appropriate insurance provider where a claim is deemed the appropriate course of action.
- ensure required details are provided to insurance provider including, but not limited to, evidence of ownership for loss and damages etc.

If insurance provider approves claim, the claim number and assessment details are sent to the AM for recording.

Asset Manager to:

- record details within the Insurance Policy Schedule Register located in the Finance files in 'O' Drive.
- record and file all documents into relevant files such as premises or fleet files depending on the insurance claim.
- be notified from the insurance provider of the reimbursement details of the claim.
- communicate with relevant employee in the Finance department of this reimbursement.

6.0 CANCELLING INSURANCE POLICY

Authorisation for cancellation of insurance policies must be approved by the MD. The only exception to this is the cancellation of motor vehicle insurance upon the sale of the vehicle.

7.0 REVIEW

Review all policies mid-year to ensure terms are maintained. Upon notification of operational changes, amend policies as required.

8.0 INSURANCE CERTIFICATES

All of the Insurance Certificates of Currency can be located in the Reference Documents section of the SQM and will be reviewed according to section 7*.0 Review*. Please contact the AM directly for all insurance certificate enquiries.

9.0 RELATED DOCUMENTS

Document Name	Document Name
Motor Vehicle Accident Claim (i050301)	Insurance Policy Schedule Register *Located in the Finance files in 'O' Drive*
Insurance Certificates of Currency *For a full list please refer to the Reference Documents section* *of the SQM.*	

10.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	23 February 2023
Effective Date	24 February 2023	**Document Number**	e310300_v2_230224

(Uncontrolled when printed)

1.13.7 Maintenance of Pool Vehicles

1.0 COMPANY VEHICLES

STEPS Group of Companies (STEPS) provides vehicles for use by managers and employees who are required to attend to work related matters including visiting and caring for clients.

1.1 RESPONSIBILITIES

The Site Manager or delegate is responsible for the condition of the pool vehicles located on their site.

Each site will conduct an inspection of the vehicle/s on a monthly basis completing either the Remote Vehicle Inspection Form (i051001) or the Pool Vehicle Inspection Form (i051003).

Once either the Remote Vehicle Inspection Form (i051001) or the Pool Vehicle Inspection Form (i051003) has been completed, this form is to be saved in the following location:

'O' Drive > WHS > (relevant site location) > Fleet Vehicles

Sites will also ensure pool vehicles have access to seatbelt extenders, when applicable, seat covers and incontinence products if required.

The Site Manager or delegate will arrange servicing for all pool vehicles or any other maintenance required as a result of the vehicle inspection/s.

Where a vehicle has been involved in an accident or unknown damage has been identified, it must be documented on the Motor Vehicle Accident Claim Form (i050301) and a copy forwarded to the Asset Manager. The Asset Manager in consultation with the Finance Manager will determine whether to repair the damage via insurance or an independent contractor depending on the level of damage and cost to repair. Site Managers or delegates may make recommendations to the Asset Manager for a pool vehicle to have minor damage repaired if the appearance does not meet the organisations corporate image.

The Site Manager or delegate will ensure that all site vehicles are booked using the Smartrak online booking system. At sites where there is no Smartrak Keymaster vehicle keybox, vehicle keys are to be collected and returned to a vehicle key custodian who must check the vehicle in and out when issuing and receiving the keys. The Site Manager or delegate will arrange for pool vehicles to receive a standard detail once a month at the expense of STEPS.

If a pool vehicle at a site is not going to be utilised for a period of time, the Site Manager or delegate will notify the Asset Manager so that arrangements can be made for the vehicle to be relocated and utilised at another site for this duration.

2.0 RELATED DOCUMENTS

Document Name	Document Name
Motor Vehicle Accident Claim Form (i050301)	Pool Vehicle Inspection Form (i051003)
Remote Vehicle Inspection Form (i051001)	

3.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	6 April 2023
Effective Date	21 April 2023	**Document Number**	i051000_v4_230421

(Uncontrolled when printed)

1.13.8 Cash Float

1.0 INTRODUCTION

STEPS and its related entities and brands will ensure that cash floats are established and managed appropriately where the business offers cash as a payment option to customers. This may include cash floats for one off events.

1.1 DEFINITIONS

Cash Float	Agreed amount of cash funds kept in the cash drawer to enable change to be provided to customers paying by cash.

Cashier	Employee responsible for cash float.

2.0 PURPOSE OF CASH FLOATS

Cash floats are only to be used for business and activities connected to STEPS activities.

Cash floats are to be used to provide change for customers paying in cash, and only where cash is accepted within the business. This may include the float being established for one off STEPS events.

3.0 INAPPROPRIATE USE OF CASH FLOATS

Cash floats are NOT to be used in any circumstances for purchasing any items or goods. It is inappropriate for cash floats to be used in any of the following circumstances:

- Purchase of any items or goods
- Cashing cheques
- Temporary loans or salary advances
- Payment of creditor accounts
- Labour services. For example; individuals should not be paid cash for work performed
- Travel related expenditure. For example; fuel, accommodation, taxi fares and travel allowances. Individual parking fees may be claimed.

If employees need to purchase goods or services that fit within any of the categories above, they should refer to the Procurement Procedure (i030100).

4.0 SEGREGATION OF DUTIES

A Cashier may not issue cash to themselves under any circumstances and approve their own claim. The claim must be approved by their Manager.

5.0 CASHIER AND FLOAT ESTABLISHMENT

A Cashier must be appointed by the appropriate manager to manage each cash float.

Multiple people including the Site Manager may be authorised to be a Cashier (to provide cover) but only one Cashier can have control of the cash float.

The Cashier is responsible for:

- Securing and limiting access to cash funds
- Reconciling the cash float daily
- Notifying Finance of any change in the account (e.g. theft).

Employees who have not been formally appointed as Cashier are not authorised to manage a cash float, even on a temporary basis.

The float can be created at the same time as establishing a Cashier.

It is the responsibility of the Chief Financial Officer (CFO) to approve the establishment of a float.

It is the responsibility of the Finance Department to process the float amount through the finance system and ensure that bank signatories are updated.

6.0 CHANGE TO CASHIER (ABSENCE, CHANGE OF DUTY, RESIGNATION)

Where a Cashier will be absent for a period, has changed responsibilities, or has left the organisation, the Manager (or pre-approved Cashier) must immediately complete a Cash Handover Form (e310101) and submit it to the Finance Department.

It is the responsibility of the Finance Department to advise that bank of any change in authorised signatories.

7.0 SAFEGUARDING CASH

The Cashier is responsible for ensuring the safeguarding of the cash float.

When not in use, the cash float should be kept in a locked till or cash register, in a locked safe or cabinet.

Where possible, the storage area should be away from large traffic flows and from areas open to public view.

Keys to the cash register or cabinet should be stored securely (not openly on the Cashier’s desk or in their desk drawer).

8.0 STOLEN OR LOST CASH FLOATS

If cash funds are stolen or a reconciliation difference is found due to incorrect change provided to a customer, or the Cashier has reason to suspect fraudulent or irregular transactions, they must notify both their Manager and the CFO immediately.

9.0 ADMINISTERING THE CASH FLOAT

At all times the total of cash in a till or cash register must be equal to the cash float value, plus the value of any unbanked cash sales since the previous banking date.

The till or cash register must be reconciled each trading day.

Cash sales are to be counted and provided to the Finance department to be banked at least weekly.

10.0 END OF FINANCIAL YEAR RECONCILIATION

At the end of the financial year (30 June) all cash floats should be reconciled by the Cashier and the Cash Float Year End Certification Form (e310103) completed and returned to Finance Team no later than 5 July each year.

11.0 RELATED DOCUMENTS

Document Name	Document Name

Cash Float Year End Certification Form (e310103)	Cash Handover Form (e310101)
Procurement Procedure (i030100)	Register of Suppliers and Contractors (i030101)

12.0 GOVERNANCE

Document Owner	Chief Financial Officer	**Approval Date**	25 July 2024
Effective Date	30 July 2024	**Document Number**	e310100_v2_240730

(Uncontrolled when printed)

1.13.9 Procurement

1.0 INTRODUCTION

This procedure outlines the procurement controls STEPS Group of Companies (STEPS) will use to manage the purchase of products.

1.1 DEFINITIONS

Products	Refers to Goods and Services
Dangerous products	High Risk Electrical and / or fuel powered equipment. Services that a reasonable person would determine to be risky.
Provider	Refers to Suppliers and contractors (Trade Contractors, Service Contractors and Independent Contractor).
Suppliers	Provide goods.
Trade Contractors	Provide a trade service (including but not limited to, shop fitting, plumbing, building, electrical, tree lopping, ICT installers).
Service Contractors	Provide a non-trade service (including but not limited to Consultants, Independent Contractors eg NPA assessors, 3rd party SEE providers).
Independent Contractors	A subset of service contractors who deliver our programs (including but not limited to NPA Independent Contractors, 3rd party SEE Sub-Contractors, HACC)

2.0 PURCHASE OF PRODUCTS

The following principles must be adhered to: value for money, open and fair competition, accountability, risk management, probity and transparency. In keeping with STEPS' commitment to Indigenous Procurement, it is important to seek opportunities to engage Indigenous businesses in the procurement process.

To ensure value for money STEPS will purchase from Providers who offer the most suitable product at the most reasonable price. All purchases must be made in accordance with the Delegations Register (i010601).

Where a single purchase is over $10,000 (excl. GST), or is a dangerous product, the provider will be subject to STEPS WHS, quality and environment performance criteria to ensure they meet regulatory and AS4801 standards to ensure only **approved** providers are engaged. Approved providers are listed on the Register of Providers (i030101).

For purchases over $100,000.00 STEPS may undertake a tendering or bid process.

Purchases with a value of less than $10,000 (excl. GST) that are not dangerous products may be procured within the delegated authority, as detailed in section 6.

Only employees with appropriate delegated authority, as documented in the Delegations Register (i010601) may initiate the engagement of a provider.

All employees involved in purchasing activities are reminded of their obligations under the Code of Conduct and Ethical Behaviour (e210007) and Conflict of Interest Procedure (i010500).

3.0 MAINTAINING REGISTER OF PROVIDERS

3.1 REGISTER OF PROVIDERS

STEPS' Quality Assurance & Risk Team will maintain a Register of Providers (i030101) listed below.

3.2 WHO IS ON THE REGISTER

- Trade Contractors
- Independent Contractors for our program delivery(excluding NPA Assessors) (5.0)
- Other providers determined during annual finance review (i.e. Purchases over $20,000 pa) (7.0)
- Providers where a single purchase is greater than $10,000 (4.0)
- Providers of dangerous products (4.0)
- Providers who have been rejected or withdrawn.

3.3 WHO IS NOT REQUIRED TO BE ON THE REGISTER

- Service contractors not falling into any other category e.g. ($10,000 single purchase or $20,000 in the year)
- Any procurement Under $10,000 and not electrical or dangerous products

3.4 PROVIDER EVALUATION

If the provider is a Trade or Independent Contractor, a Trade & Independent Contractor Information Form (i030102) must be completed.

The completed forms and Contractor Insurance Certificates must be returned to the Quality Assurance & Risk team via email to Quality Team inbox to record on the Register of Providers (i030101).

Insurance Certificates are located under O:\Corporate Admin \ Register-Providers-Insurance

3.5 STATUS

The status of evaluation for each supplier and contractor will be stated as:

- “A” for approved.
- “W” for withdrawn.
- “R” for rejected (Any name with a “W” or “R” against it must not be used).
- “N” not in use

Where the name is tagged with a “W” (for withdrawn) or “R” (for rejected), the provider must not be engaged unless there is strong evidence to suggest recent major improvements in their WHS, quality and environment practices and then a re-assessment is required. This must be approved by ELT.

Requests to update the Approved List can be done by employees by providing a Change - Register Status Form (i030104) to the Quality Assurance & Risk team to the Quality Team inbox .

3.6 REVIEW OF REGISTER OF PROVIDERS

The Register of Providers (i030101) will be reviewed by EMT annually in March. Where a contractor is not to be retained, they shall be withdrawn from the Register of Providers (i030101). The Quality Assurance & Risk Team will forward the Register of Providers (i030101) to the Chief Finance Officer (CFO) February of each calendar year to be reviewed at the March EMT meeting. The Quality Assurance & Risk team will amend the register and ensure the withdrawn contractors are tagged with a “W” to denote withdrawal from the Register of Providers (i030101).

3.7 REASSESSMENT OF A PROVIDER

If the appropriate Manager is of the opinion that the performance does not meet satisfactory standards, the Change - Register Status Form (i030104) must be completed by the Manager and forwarded to the Finance Department.

Where a Provider is to be removed from the Register of Providers (i030101) or placed back on the Register of Providers (i030101), the person requesting the approval shall submit their case to the EMT. If agreed by the EMT, the required amendments will be made to the applicable register by submitting a Change - Register Status Form (i030104) to the Quality Assurance & Risk team.

4.0 THE PROCUREMENT PROCESS FOR PRODUCT OVER $10,000 OR DANGEROUS PRODUCT.

4.1 SELECTION OF PRODUCT

Consider the following:

- Technical specifications and requirements to ensure quality, WHS and environment impacts are acceptable to STEPS (usually satisfied if product complies with Australian Standards).
- Are there warranties and/or certificates.

4.2 SELECTION OF PROVIDERS

To ensure risks in the workplace are eliminated or minimised all employees seeking to engage a provider, must take into account and weigh up all relevant matters, including:

- Does the provider have the ability to meet product specifications and time frames.
- References, referrals, or industry feedback regarding the standard of work, reliability, delivery performance.
- Length of time in business, skills, and extent of workforce for the size of the job, type of equipment utilised, and standard of work displayed.
- Samples of product for evaluation, if available.

5.0 ENGAGING INDEPENDENT CONTRACTORS

Prior to entering into:

- an Independent Contractor Agreement; or
- Service Agreement.

The Independent Contractor must complete the Trade & Independent Contractor Information Form (i030102) and provide a copy of current insurance certificates (Public liability, Workers Compensation or Professional Indemnity) as relevant.

If insurance certificates are provided and WHS requirements satisfied, the terms of the relationship need to be documented with the relevant Agreement and a Contractor Deed of Confidentiality (i030106) signed. All contracts including the Contractor Deed of Confidentiality (i030106) must be signed by the Managing Director. Once documents are executed all documentation pertaining to the Independent Contractor, including agreements, insurance certificates and completed Trade & Independent Contractor Information Form (i030102) will be forwarded to the Managing Directors Executive Assistant who will file the documentation and provide the Trade & Independent Contractor Information Forms and Insurance Certificates to the Quality Assurance & Risk Team.

6.0 PROCUREMENT LESS THAN $10,000 (EXCL GST)

Procurement that has a value of less than $10,000 (excl GST) and is not dangerous goods may be secured within the delegated authority.

STEPS only provides a purchase order when requested by the supplier. When a supplier requests a purchase order, the employee must complete the *Purchase Order Request Form (Outlook Form),* obtain managerial approval and forward to Finance, who will create and transmit the purchase order as per the outlook request.

7.0 EVALUATING PROVIDERS (Total annual purchases >$20,000)

In addition to the review of the register, Providers will be evaluated by the Finance Department where a supplier has provided goods or services in excess of $20,000 in the previous financial year. Excluded from this review will be landlords, NPA Assessors, Utility companies, Banks, Superannuation funds. The evaluation outcomes will be documented on the Change - Register Status Form (i030104).

Any provider that is evaluated under this paragraph, shall be recorded on the Register of Providers (i030101) by the Quality Assurance & Risk team.

8.0 RELATED DOCUMENTS

Document Name	Document Name

Register of Providers (i030101)	Trade & Independent Contractor Information Form (i030102)
Change - Register Status Form (i030104)	Contractor Deed of Confidentiality (i030106)
Purchase Order Request Form (Outlook Form)	Conflict of Interest Procedure (i010500)
Delegations Register (i010601)	Code of Conduct and Ethical Behaviour (e210007)

9.0 GOVERNANCE

Document Owner	Chief Financial Officer	**Approval Date**	18 November 2021
Effective Date	17 December 2021	**Document Number**	i030100_v4_211217

(Uncontrolled when printed)

1.13.10 Purchasing Gift Cards Procedure

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) have the need in some circumstances to issue Gift cards to assist the students, participants and clients (clients) it supports. These gift cards will be issued as eGift cards (electronic gift cards).

The purpose of this procedure is to establish clear and definite guidelines on who is able to purchase these gift cards, how and who these are issued to, and how these are recorded and reconciled.

2.0 PURPOSE AND MONETARY LIMITS

STEPS will only issue gift cards that cannot be used to purchase alcohol or tobacco products. Primarily, the gift cards issued will be the Woolworths Fuel and Essentials and/or Coles Groceries gift cards. Other gift cards may be issued where a Woolworths and Coles are not available, or the assistance being provided for is not supplied under these gift cards.

Gift cards may be issued to clients for:

- Student attendance incentives (SEE/AMEP)
- Student and client support as per contract guidelines (Skilling Queenslanders for Work – SQW, IRSP, GRSP)
- Travel assistance (DES, SQW, Schools Out Works In, IRSP, GRSP).

The maximum gift card limit is $25 in each instance. Gift cards of a higher value must be approved by the relevant Contract Manager or General Manager.

Gift Cards are not to be used as a replacement to the client reimbursement process. Reimbursements continue to be processed through the expenses approval process in ProSpend.

3.0 FINANCE DEPARTMENT RESPONSIBILITIES

The Chief Financial Officer (CFO) is responsible for the operation and control of the gift card process.

The CFO and Finance Manager will coordinate the issuing of gift cards upon receipt of the approved gift card request. To reduce administration, these gift cards will be issued directly to clients wherever possible.

Any pre-ordered gift cards will be stored securely with limited access to the gift cards. A reconciliation of held and issued gift cards will be undertaken at least monthly, and at every time a gift card order is placed.

A maximum of twenty (20) gift cards or maximum value of $500 can be preordered and held at any one time to enable responsive turnaround times to gift card requests, and to take advantage of discounts offered for bulk orders. Any pre-ordered gift cards stored by the Finance Department will be in denominations of $25 as this is the most widely used denomination.

Gift cards will not be purchased on corporate credit cards, either through the finance team or Managers at sites.

Permissions and access to O Drive gift card folders are approved by the CFO or Finance Manager, and only upon receipt of the gift card administrator request form.

4.0 GIFT CARD REQUESTS

Requests for gift cards to be issued must be received on the Outlook Gift Card Request form. This correctly completed form must be approved in line with the delegations register. Where the gift card request exceeds $25 for a client in any one instance, this must be approved by the relevant Contract Manager or General Manager.

Where the request is for more than one gift card (for example for the issuing of student attendance incentives), the gift card request may be submitted with a supporting Gift Card Bulk Order (e310502). The overall value of the gift card request must be within the approved delegation of the approver.

A site may hold six (6) gift cards on site at any one time to enable prompt/emergency issuing of gift cards to clients. The issuing of these gift cards must only occur upon approval of the Manager, using the Outlook Gift Card Request form as per other gift card requests. A copy of this approval is to be forwarded to the Finance Department. These held gift cards will be required to be reconciled on the site gift card register prior to any requests of further gift cards or issuing of further gift cards.

Requests for gift cards should be preplanned wherever possible to enable the purchase, receipt and issuing of gift cards in a reasonable timeframe. It is expected that the process will result in a turnaround time of no more than 5 business days.

5.0 SEGREGATION OF DUTIES

An employee may not request and approve the gift card request. Where the gift card request is being submitted by a manager, their manager must provide the approval (no self-approval will be accepted).

Within the Finance department, at least two people must be involved in the ordering, issuing gift cards and invoice approval process to ensure segregation of duties. No one person can undertake each of these tasks.

6.0 GIFT CARDS ADMINISTRATOR

The Business Manager is the appointed administrator at each site.

A site may require more than one administrator for period of leave to ensure coverage, however only one administrator will have control of the gift cards at any one time.

An administrator will be responsible for:

- Securing and limiting access to gift cards
- Keeping records of the gift cards on the gift card register
- Monitoring gift card requests to ensure they comply with the purchasing gift cards procedure
- Confirmation that the gift card register has been reconciled monthly to the finance team.

To nominate a gift card administrator for leave coverage, the Manager and proposed administrator must complete a Gift Card Administrator request form and submit it to the Finance Department.

7.0 CHANGE TO GIFT CARD ADMINISTRATORS

Where an administrator will be absent for a period, has changed responsibilities, or has left the organisation, the manager (or pre-approved alternate Administrator) must immediately complete the Gift Card Administrator Handover (e310504) and send to the Finance Department.

8.0 SAFEGUARDING GIFT CARDS

Gift cards must be stored in an electronic location only accessible by the Manager, approved Gift Card Administrators and nominated Finance Team members. The ICT team will assist with an appropriate O drive folder set up.

To reduce the risk of gift cards on site, only six (6) unused gift cards should be stored at any one time. Wherever possible gift cards will be issued directly to clients by the Finance Department.

A reconciliation must be kept of all gift cards for each site on the sites gift card register. The Finance Department will issue a gift card register for each site.

9.0 ADMINISTERING THE GIFT CARD REGISTERS

The gift card administrator is responsible for maintaining the gift card register for the site. At all times the gift card register must be kept current with all gift card requests and gift cards issued. The gift card register will include instructions on how the gift card register is to be maintained and the required detail to be captured in the gift card register.

These registers will be used for the monthly reconciliation of gift cards held by STEPS.

10.0 END OF FINANCIAL YEAR RECONCILIATION

At the end of the financial year (30 June) all gift card registers are to be reconciled by the administrators and the Gift Card Year End Certification (e310503) completed and returned to the Finance Department no later than 5 July each year.

11.0 RELATED DOCUMENTS

Document Name	Document Name
Appointment of Site Gift Card Administrator Request (e310501)	Gift Card Administrator Handover (e310504)
Gift Card Bulk Order (e310502)	*Gift Card Register (available from Finance Team)*
Gift Card Year End Certification (e310503)	*Outlook Gift Card Request form*

12.0 GOVERNANCE

Document Owner	Chief Financial Officer	**Approval Date**	11 July 2024
Effective Date	16 July 2024	**Document Number**	e310500_v1_240716

(Uncontrolled when printed)

1.14 Marketing and Communications

The communications team is dedicated to ensuring that all of STEPS publications and communications material (printed and online) is of a high standard and represents our brand consistently and effectively.

STEPS visual identity is an important part of our image. This image is expressed not only in our logo and colours but also in all of our printed and online materials through the language, layout and tone that is used, as well as at our sites through the signage, display and promotional material on show.

Frequently used forms are listed below, for all other related Procedures & Documents refer to the Marketing and Communications Chapter link

Authority to Release Information - Media- Customers (e340021)

Authority to Release Information (Media) - Staff/Volunteer (80102)

Business Card Order Form (e340020)

1.14.1 Activity and Event Management

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has a strong commitment to creating an exceptional service platform for our customers. Use of the Activity / Event Management Form will enable effective planning and management of activities and events with due consideration to budget, resource allocation and approvals.   Resources can be limited for many reasons, therefore planning and well organised activities and events increase the potential for success of the activity or event and improved quality of communication between teams.

For activities and events to be conducted at the George Street, Caloundra site that require catering, please complete the Cafe on George - Catering Order Form.

These procedures are not to be confused with the Project Management Framework which is designed to address Strategic and Operational projects that are not considered to be business as usual.

1.1 DEFINITIONS

Activity	Fits within business as usual; the introduction of a new activity, group or expo to accomplish a skill, maintain partnerships, and provide a safe environment for social interaction, inclusion or education.
Event	An event is a planned public or social occasion / function where guests are invited to participate in proceedings that are coordinated by STEPS.
Peer Worker	An individual appointed with a specific role in sharing their lived experience with others in order to educate, support and / or inspire.

2.0 ACTIVITY / EVENT PRE-PLANNING

2.1 PRELIMINARY ASSESSMENT

Prior to starting a proposal or to gain approval for any future activity or event the person/s responsible for planning and organising the activity or event are to research and consider the following factors:

- Objectives – How does the proposed activity / event align with STEPS' strategic goals and objectives?
- Relevance – How does the proposed activity / event align with STEPS' current organisational business streams? How would the proposal support programs, activities or events that we are currently delivering?
- Customer Feedback – How does the proposed activity / event support feedback from our customers / stakeholders regarding what they would like to see at our future activities or events, or ideas for new activities or events?
- Work Health and Safety (WHS) and Risk – What are the workplace health and safety and operational risks that need to be considered? How will they be mitigated?

2.2 PEER WORK AT EVENTS OR ACTIVITIES

Having Peer Workers involved in events and activities is consistent with elements contained in Standards against which STEPS is certified, as this demonstrates partnering with consumers and encouraging client participation.

STEPS may seek to have an individual with lived experience support an event or activity by asking them to provide:

- Education from a lived experience perspective
- Inspire others by sharing stories of recovery
- Assisting in health promotion and wellbeing activities
- Supporting research or evaluation among different age groups or culturally and linguistically diverse communities

Often the role of peer work is voluntary, and generally not paid. STEPS should always consider how best to provide acknowledgement of peer involvement and compensate the person for their efforts and participation.

At a minimum the person should be reimbursed any expenses to attend the event or activity. Payment in the form of cash or gift cards would need to be approved by the Managing Director (MD) / Chief Executive Officer (CEO). This should occur before approaching the person to ensure that any compensation is equitable and fair.

If a formal agreement (i.e. a service agreement MOU) is to be entered into please refer to the Contract Acceptance and Execution Procedure.

3.0 ACTIVITY / EVENT APPROVAL PROCESS

To enable each activity / event to succeed it is important that comprehensive planning and communication is managed prior to the occasion and that a review of outcomes is conducted upon conclusion of the activity / event.

The Activity and Event Management form has been designed to support the end to end process of an activity / event's lifecycle.

3.1 THE ACTIVITY / EVENT PROPOSAL

The first section of the form is the Proposal which is designed to enable approval by the ELT member prior to approval by the MD / CEO (or their delegate) before detailed planning commences. It is also to be used to co-ordinate with other departments to ensure they can accommodate any request for assistance and / or involvement in a timely manner.

3.2 THE ACTIVITY / EVENT PLAN

The second section requires detailed information to be gathered to enable formal approval of the activity / event. The Plan is to be completed in full prior to being submitted to an ELT member for their review. Formal approval of the activity / event must be obtained from the MD / CEO prior to initiating actions or incurring expenses associated with the activity / event.

3.3 THE ACTIVITY / EVENT REVIEW AND REPORT

The third section of the form is a review of the activity / event comparing the planned outcomes with the actual outcomes. The review is to be completed within one week of the activity / event being conducted. The completed form is to be submitted to an ELT member for review. Depending on the actual outcomes of the activity / event the ELT may require further investigation / analysis or actions to be conducted to improve outcomes for future activities / events.

3.4 WHS AND RISK ASSESSMENTS

Where necessary, risk assessments must be conducted on the proposed activity or event to ensure that controls and / or specialised equipment that may be required can be organised beforehand. Please refer to the Risk Management Procedure for full details on identifying hazards and conducting risk assessments.

4.0 EVENTS CALENDAR SCHEDULING

4.1 PURPOSE

In order to maximise customer involvement and provide quality information it is essential STEPS' activities and events are scheduled in advance to enable comprehensive and safe co-ordination of all actions, details of the activity / event are to be communicated and shared on appropriate platforms via the relevant channels to nullify any potential clashes within STEPS' or other organisations' planned activities / events.

Once an activity / event date has been determined and authorised via the approval process, all activity / event details are to be provided to the Marketing and Communications Team for populating into the Events Calendar.

5.0 RELATED DOCUMENTS

Document Name	Document Name
Activity / Event Management Form (i011001)	Cafe on George - Catering Order Form (5030001)
Contract Acceptance and Execution Procedure (i010900)	Risk Management Procedure (i050100)

IMS_i011000_ActEvntMgmt_v6_240916_7744

(Uncontrolled when printed)

1.14.2 Award Nominations

1.0 INTRODUCTION

This procedure will ensure all award nominations and processes are conducted professionally and strategically to effectively promote and protect the identity of the organisation, while supporting and promoting the expertise of team members who are deserving of an award of recognition.

STEPS Group of Companies (STEPS) is committed to presenting a professional image to its customers, stakeholders and the general community when nominating for awards by using accurate and timely information provided in any award process to minimise the incidence of incorrect or inappropriate information being shared.

STEPS coordinates proactive and responsive nominations for relevant sector, professional, community and business awards. This requires all employees to adhere to a consistent approach to award nominations and submissions, including publicity and media liaison.

1.1 OBJECTIVES

- To improve and enhance STEPS' profile by professionally seeking and responding to award nominations opportunities
- To ensure all information provided to award and statements by nominees support STEPS' vision, policies and strategic priorities
- To assist senior management in planning for and dealing with enquiries and issues arising from award nominations or successes
- To streamline and systemise STEPS' procedures for preparing, approving, distributing and recording appropriate, newsworthy and correct public information.

2.0 APPROVAL PROCESS

All nominations for professional, community or other awards which involve, reflect or are based on an employee's paid role with STEPS, whether by employees who self-nominate for an award or nominations made by others, must be advised to and endorsed by the employee's direct reporting Manager.

Any conflict of interest must be declared to the employee's direct reporting Manager. Refer to Conflict of Interest Procedure (i010500) and Conflict of Interest Disclosure (i010501).

Employee's nominated for any awards based on their role must have the full authorisation and support of the Managing Director (MD).

Employees may not proceed and participate in any award process that involves discussion of their employment, role or responsibilities for STEPS without this approval.

It is not appropriate at any time for any employee to provide an external person, committee or organisation with information about STEPS without prior authorisation. This includes participating in an award process and providing personal anecdotes, experiences or viewpoints about an employee's role within STEPS.

3.0 NOMINATIONS

All award nominations are to be handled promptly, efficiently and courteously. On first contact, employees must provide the information to their Manager for consideration. If the manager endorses the nomination, approval will be sought from the MD (as stated in 2.0).

All employees are required to supply appropriate information in a timely manner to enable an official response.

At certain times, e.g. when more than one employee is nominated, the organisation may decline for an employee to participate in the awards process. In any situation of doubt, the MD is the ultimate arbiter in relation to the approval of participation in an awards process.

The Customer Success Manager (CSM) will assist with preparation of appropriate, official information about the organisation and may refer submissions to other senior managers for input and validation, e.g. regarding financial, human resources or technical information.

All information or submissions provided to an awards process must be consistently formatted and clearly identify STEPS' logo and contact details, as approved by the MD and relevant Manager.

4.0 MEDIA

Media information will be prepared for checking and final approval by the MD.

If information or an interview with media is required, employees must refuse permission to be quoted as the spokesperson for STEPS and instead request that the journalist quotes either the supplied media information or the relevant, approved STEPS spokesperson.

An award nomination or success is not valid reason for any employee to provide information about STEPS to media, the general public or an awards committee or organisation.

5.0 CONDITIONS

Employees, volunteers or other paid workers of STEPS may self-nominate or be nominated for a relevant professional, community or other award if each of the following criteria is met.

- Self-nomination by an employee is discussed in advance with a relevant Manager and is permitted for one category only of any award.
- Any employee nominated for an award must be currently employed by STEPS, nominated for the most relevant award category and they must have worked for STEPS for at least one calendar year.
- Nominations of an employee by another employee of STEPS is required to be confirmed by the MD prior to proceeding with any awards process.

The criteria to be assessed and confirmed by the Managing Director as relevant for an employee's self-nomination for an award may include:

- significance and impact of contributions made by the employee to date
- demonstrated level of commitment to the betterment of STEPS and its customers
- degree of difficulty of the achievement
- nature and length of activity or service
- future goals and likely impact on STEPS, customers and communities
- previous awards and recognition received
- demonstrated excellence in their field
- whether his or her contribution was in the course of employment, voluntary or both
- personal attributes of the nominee such as being an inspirational/positive role model, showing vision, leadership, innovation and creativity
- Personal, academic and professional achievements.

6.0 ACCESS TO STEPS PROPERTY

Awards, media or community representatives are not permitted in non-public areas of any STEPS offices, sites or property without prior approval and protocols for access must be followed, including escorting at all times by an employee to provide them every assistance.

7.0 RELATED DOCUMENTS

Document Name	Document Name
Conflict of Interest Disclosure (i010501)	Conflict of Interest Procedure (i010500)

8.0 GOVERNANCE

Document Owner	Managing Director	**Approval Date**	13 July 2023
Effective Date	14 July 2023	**Document Number**	e340300_v2_230714

(Uncontrolled when printed)

1.14.3 Media Relations

1.0 INTRODUCTION

STEPS is a national for purpose organisation committed to presenting a professional image to its customers, stakeholders and the general community by coordinating proactive and responsive media relations, including publicity and media liaison to promote and protect its image.

The purpose of this procedure is to consistently ensure that the most accurate and timely information is available to the media, and thereby the public, and to minimise the incidence of incorrect or inappropriate information being released.

1.1 DEFINITIONS

Media	Newspapers, magazines, journals, bulletins, newsletters, radio programs, television programs, electronic media and social media.
Journalists	Representatives of media organisations, including reporters, researchers, managers and technical staff external to the organisation.

1.2 OBJECTIVES

- To improve and enhance STEPS profile by professionally seeking and responding to positive media opportunities;
- To ensure all media contact and statements support STEPS Commitment, Values, policies and strategic priorities;
- To provide media with approved contact points for STEPS (approved by the Managing Director [MD]);
- To provide approved and consistent messaging;
- To streamline and systemise STEPS procedures for preparing, approving, distributing and recording appropriate, newsworthy and correct public information; and
- Processes and relevant employee authorities are outlined for providing strategic information to media for sharing and to inform their own understanding of STEPS.

2.0 MEDIA ENQUIRIES

All media enquiries for publicity, e.g. news stories, feature articles or industry comment, are to be directed to the Marketing and Communications Manager (MCM). When the MCM has ascertained the information request, the MD and appropriate employees will be contacted to gather information and relevant advice for an official statement.

All media enquiries are to be handled promptly, efficiently and courteously. Media are to be advised of a preferred contact who will provide the official response in consultation with the MCM.

Information and issues which merit media coverage are to be directed to the MCM for development of approved releases or statements for media liaison.

2.1 AUTHORISATION AND APPROVAL

Authorisation of media releases, statements, responses to media enquiries and other media activities are to be authorised by the MD and MCM.

All official comments and strategic advice for media relations can only be provided by the MD.

The MCM can provide official information relating to STEPS as a whole, corporate issues and general STEPS activities as approved by the MD.

STEPS employees are not authorised to provide media responses or general comment, except with the prior approval of the MD. This approval may be sought if an employee has been identified in a media release or by media contact as a spokesperson for a specific issue. Employees may then supply facts but are not authorised to offer opinions on behalf of STEPS. When such authority is given, all statements must be coordinated through the MCM.

Breaches of this procedure by employees may be considered to be breaches of the Code of Conduct and Ethical Behaviour and may result in disciplinary action.

3.0 MEDIA ACCESS TO PREMISES

Media representatives are not permitted in non-public areas of any STEPS offices, sites or property without the prior approval of the MD or MCM and must be escorted at all times by an employee to provide them assistance.

4.0 RELATED DOCUMENTS

Document Name	Document Name
Code of Conduct and Ethical Behaviour (e210007)	Social Media Procedure (e210200)

SE_e340200_MedRelations_v2_240913_6963

(Uncontrolled when printed)

1.14.4 Social Media

1.0 INTRODUCTION

STEPS Group of Companies (STEPS) has developed this procedure in recognition of the significant participation of employees in social media.

For employees who use social media either as part of their job or in a personal capacity, it is important to understand an employees' obligations when the online communication is about STEPS, our products and services, employees or other work-related issues.

It is also important to note that behaviour on social media sites is still bound by the Code of Conduct and Ethical Behaviour (e210007) and the Deed of Confidentiality and Restraint (i070107) (even outside work hours).

1.1 DEFINITIONS

Social Media	The term ‘social media’ refers broadly to any online media which allows for user participation, interaction or publishing. Commonly used social media tools include, but are not limited to, Facebook, YouTube, Twitter, LinkedIn, Tik Tok, Instagram, blogs, forums and wikis.

1.2 RESPONSIBILITIES

Executive Leadership Team:

- Promote and model behaviour consistent with this procedure
- Ensure employees are aware of their responsibilities as outlined in this procedure.

Supervisors:

- Must address any suspected breach of this procedure and/or discuss the matter with the Human Resources team.

Employees:

- Are responsible for their own communications online
- Must make sure comments made are not, and could not be perceived to be made on behalf of STEPS, rather than an expression of a personal view
- Should refer to their manager if they become aware of potential breaches of this procedure
- Must comply with STEPS policies and procedures and Deed of Confidentiality and Restraint (i070107).

1.3 APPLICATION

This procedure applies to all employees, contractors and volunteers of STEPS.

This procedure does not apply to:

- Employees’ personal use of social media where no reference is made to STEPS and/or such usage has no connection to the workplace or work-related matters; or
- Online communications published by STEPS representatives who are specifically authorised to communicate via social media platforms on behalf of STEPS.

2.0 PERSONAL USE OF SOCIAL MEDIA

Although many users may consider their personal comments posted on social media or discussions on social networking sites to be private, these communications are frequently available to a larger audience than the author may realise.

As a result, any online communication that directly or indirectly refers to STEPS, our products and services, employees or other work-related issues, has the potential to damage STEPS' reputation or interests.

When participating in social media in a personal capacity, employees must:

- Not disclose STEPS' confidential information, proprietary or sensitive information. Information is considered confidential when it is not readily available to the public.
- The majority of information used throughout STEPS is confidential. If you are in doubt about whether information is confidential, refer to the Code of Conduct and Ethical Behaviour (e210007) and/or ask your Manager before disclosing any information.
- Not use the STEPS logo or company branding on any social media platform without prior approval from the Marketing and Communications Manager;
- Not communicate anything that might damage STEPS' reputation, brand image, commercial interests, or the confidence of our customers;
- Not post any material that would directly or indirectly defame, harass, threaten, discriminate against or bully any STEPS employee, client or customer;
- Ensure, when identifying themselves (or when they may be identified) as a STEPS employee, that their social media communications:
    - Are lawful; and
    - Comply with STEPS' policies and procedures including the Code of Conduct and Ethical Behaviour (e210007), Anti-Discrimination and Equal Opportunity Policy (i010102) and Acceptable Use Policy (6001700).

3.0 GOOD PRACTICE WHEN USING SOCIAL MEDIA

When engaging on social media, employees should:

- Exercise care and discretion with their use of online communication. Employees should work on the assumption that content may be viewed by, sent, forwarded, or transmitted to someone other than who was intended to view the communication;
- Take care not to disclose other people's personal information or publish images of others without permission. Be aware that people may be readily identifiable even when names are not used;
- Refer to their Manger if unsure whether an intended online communication may be in breach of this procedure;
- Use common sense and respect others in posts and discussions. If an employee disagrees with the opinion of another, they should keep responses appropriate and inoffensive;
- Adopt the simple practice of stepping back, re-reading and thinking about what they post before doing so.
- Carefully review the privacy settings on your account to reduce the chance of mistaken posts being seen.
- Review the Terms and Conditions of usage before using any site.

4.0 EXAMPLES OF POTENTIAL BREACH

Examples of potential breaches of this procedure include but are not limited to:

- Posting a comment on the STEPS Facebook page in response to a customer comment or complaint;
- Uploading video footage to YouTube showing anything that could damage STEPS' reputation;
- Making derogatory comments about STEPS or STEPS' employees, customers or clients;
- Posting obscene images or offensive comments to Facebook about a work colleague where this could constitute bullying, discrimination or harassment;
- Posting a photo or comment that may identify a customer either by name or characteristics without their consent

5.0 BREACH

Breach of this procedure may lead to disciplinary action, which may range from a warning up to termination of employment, depending on the severity of the breach. If you breach the law, you may also be held personally liable.

6.0 RELATED DOCUMENTS

Document Name	Document Name
Code of Conduct and Ethical Behaviour (e210007)	Deed of Confidentiality and Restraint (i070107)
Anti-Discrimination and Equal Opportunity Policy (i010102)	Acceptable Use Policy (6001700)

7.0 GOVERNANCE

Document Owner	Marketing & Communications Manager	**Approval Date**	11 July 2024
Date of Issue	16 July 2024	**Document Number**	e210200_v2_240716

(Uncontrolled when printed)