Reference No	POL-003	Privacy and Confidentiality

Current version number	1			
Review frequency	Annually	☐	Every two years	☒
Approved by	Board	☒	CEO	☐
Date current version approved	9 June 2026			
Next review date	9 June 2028			
Applies to	The Board; CEO; all staff, contractors, consultants, volunteers (collectively referred to as team members).			

Policy context	
This policy relates to:	
Commonwealth and state legislation	*Australian Commonwealth Acts* • Privacy Act 1988 (Cth) • Australian Privacy Principles (APPs) • Health records and Information Privacy Act 2002 (Cth) • My Health Records Act 2012 (Cth) • Aged Care Act (Cth) • National Disability Insurance Scheme Act 2013 (Cth) *Queensland Acts* • Information Privacy Act 2009 (Qld) • Public Records Act 2002 (Qld) NSW Acts • Privacy and Personal Information Protection Act 1998 • State Records Act 1998
Regulatory requirements (Standards)	*Strengthened Aged Care Quality Standards* **Standard 1 The Individual** Outcome 1.2 Dignity, respect and privacy **Standard 2 The Organisation** Outcome 2.7 Information Management *Human Services Quality Standards* **Standard 1 Governance and Management** Indicator 1.7 Effective information management systems that maintain appropriate controls of privacy and confidentiality for stakeholders *NDIS Practice Standards and Quality Indicators* **Standard 2 Provider Governance and Operational Management** Information Management *National Safety and Quality Mental Health Standards for Community Managed Organisations* **Standard 1 Practice Governance** 1.14 Consumer care records and information 1.26 Privacy *National Safety and Quality Digital Mental Health Standards* **Standard 1 Clinical and Technical Governance** 1.16 and 1.17 Healthcare records 1.28 and 1.29 Privacy 1.35 Security and stability
Best practice standards	
Organisational policies	• Code of Conduct Policy • Information Security/ICT Policy • Media and Communications Policy • Information and Records Management Policy
Forms, templates and other organisational documents	• Business Continuity and Response Plan • Cyber Incident Response Plan • System and Portal Access Procedure • Privacy Impact Assessment (PIA) Procedure

	• Information and records management procedure • Client Handbook • Right to Information Request Form • System and Portal Access Change Request Form • Employment contract • Confidentiality agreement • Media Consent Form

Definitions	
Personal Information	Information or an opinion that identifies, or could reasonably identify, an individual
Sensitive information	Includes health information, racial or ethnic origin, religious beliefs, sexuality, or criminal history
Confidential information	Information disclosed in trust and not intended for further disclosure
Data Breach	An incident where personal or confidential information is accessed, disclosed, or lost without authorisation
Consent	A clear and informed agreement by an individual to the collection, use, or disclosure of their personal information

Purpose

Footprints Community is committed to protecting the privacy, dignity, and confidentiality of all individuals whose information it collects, uses, and stores. This policy outlines the principles and practices that guide our approach to information management in compliance with applicable laws and standards

This policy applies to all personal, sensitive, and confidential information managed by the organisation, including all records, whether maintained in paper-based or electronic formats.

1.0 Collection of Information

The organisation will:

- Collect only information necessary to provide services or meet legal obligations
- Collect information from the person it relates to unless it is unreasonable and impractical to do so, taking reasonable steps to inform the individual information about them is being collected
- Collect information lawfully, fairly, and respectfully
- Inform individuals why the information is being collected and how it will be used
- Obtain consent where required

2.0 Use and Disclosure

Personal and confidential information will:

- Only be used for the purpose for which it was collected, including care coordination, service delivery, safeguarding, and compliance obligations
- Support continuity of service delivery across all programs and services delivered by Footprints
- Not be disclosed without consent unless required or authorised by law, including situations involving serious risk to health and safety
- Be shared on a need-to-know basis with authorised staff, carers, service partners, or government agencies where appropriate.
- Be discussed with owners of the information or authorised nominees after sufficient identification has been established.
- Be disclosed without consent where mandatory reporting, duty of care, or safeguarding requirements apply

3.0 Storage and Security

The organisation will take reasonable steps to protect information from misuse, loss, unauthorised access, or disclosure by:

- Secure storage of paper records (locked cabinets)
- Password protected electronic systems
- Access controls based on role
- Secure disposal (shredding or secure deletion)
- Immediately revoking access for staff ceasing employment with Footprints.
- Performing regular audits of staff access.

4.0 Data Retention and Disposal

Personal and confidential information will be retained only for as long as necessary to fulfil the purposes for which it was collected or as required by law. After this period, information will be securely destroyed or de-identified in accordance with the organisation's Information and Records Management Procedure.

If Footprints Community ceases to operate, personal and confidential information will be managed, transferred, retained, or securely destroyed in accordance with applicable laws, contractual obligations, and any lawful directions relating to the organisation's closure.

5.0 Access and Correction

Individuals have the right to:

- Request access to their personal information
- Request correction of inaccurate, out-of-date, or incomplete information.

Requests will be managed in accordance with legislative requirements and where applicable using the Footprints Right to Information request form (FRM-003). Refer to Footprints Information and Records Management Procedure.

6.0 Confidentiality obligations

All staff, volunteers, students, and contractors must:

- Have either a current signed employment contract or confidentiality agreement (Appendix A) and comply with Footprints Code of Conduct
- Respect the privacy, dignity, and cultural safety of all clients
- Maintain confidentiality during and after their engagement with the organisation
- Only discuss client information in private and appropriate settings
- Report any actual or suspected privacy breaches, unauthorised disclosures, or inappropriate access immediately

All team members will receive training on privacy and confidentiality requirements at induction, and refresher training at least annually thereafter, or more frequently where legislative, regulatory, or organisational changes occur. Responsibility for ensuring

training is completed and records are maintained rests with managers and the People and Culture Team. Compliance with training requirements will be monitored as part of the organisation's governance and quality assurance processes.

7.0 Privacy Impact Assessment

The organisation will conduct Privacy Impact Assessments (PIAs) for any new projects, systems, or processes that involve the collection, use, or disclosure of personal information to ensure compliance with privacy laws and mitigate potential risks.

8.0 Data Breaches

Any suspected or actual breach of privacy or confidentiality must be reported to management immediately. The organisation will:

- Identify and contain the breach to prevent further unauthorised access or disclosure.
- Assess the nature and scope of the breach, including the types of information affected and the potential impact on individuals.
- Notify affected individuals, guardians, nominees, or advocates as soon as practicable, providing clear information about the breach and steps they can take to protect themselves.
- Notify relevant regulators or funding bodies as required by law, including compliance with the Notifiable Data Breaches scheme.
- Review and update systems, policies, and training to prevent future breaches.

9.0 Roles and Responsibilities

All workers are responsible for:

- Complying with this policy
- Collecting, accessing, using, and sharing information only as required to perform their duties.
- Reporting suspected or actual privacy breaches immediately.
- Participating in required privacy and confidentiality training.

Leaders are responsible for:

- Implementing this policy within their areas of responsibility.
- Monitoring completion of required privacy training and maintaining oversight of compliance.
- Managing access permissions to information systems according to role requirements.
- Escalating actual or suspected privacy breaches immediately to the CEO/Privacy Officer.
- Supporting investigations and corrective actions following privacy incidents.

The People and Culture Team are responsible for:

- Maintaining records of privacy and confidentiality training.
- Ensuring confidentiality obligations are incorporated into employment contracts, volunteer agreements, and onboarding processes.
- Supporting induction and ongoing training requirements.

The CEO is the designated Privacy Officer and is responsible for oversight of privacy, confidentiality, and information management practices across the organisation.
Responsibilities include:

- Ensuring organisational compliance with applicable privacy legislation, standards, and contractual obligations.
- Overseeing the management of privacy complaints, access requests, and significant privacy incidents or breaches.
- Determining whether notification to affected individuals, regulators, funding bodies, or other authorities is required following a data breach.
- Ensuring Privacy Impact Assessments are conducted where required and recommendations implemented.
- Reporting privacy risks, breaches, and compliance matters to the Board or governing body as appropriate.

The Board are responsible for:

- Providing oversight of organisational governance, including privacy and information management risks.
- Reviewing and approving privacy-related policies, procedures, and organisational controls.
- Receiving reports on significant privacy breaches, compliance issues, and improvement initiatives where appropriate.

Appendix A

Confidentiality Agreement

Date:

Parties:

1. **Footprints Community Limited** (ABN 15 100 277 492) of 213-217 St Pauls Terrace, Fortitude Valley Qld 4006 (Company) and
2. [**Contractor Name**] of [Contractor Address] (You)

You will be engaged as [position] and, in that role, may access or develop confidential information of the Company.

Confidential Information

"Confidential information" includes, but is not limited to:

- Marketing, development plans, pricing and business strategies
- Employee and client records both paper and electronic
- Supplier names, agreement, and operational details
- Service-related data, plans, and training materials
- Information disclosed to the Company under non-disclosure from third parties

Excludes information that:

- Is publicly known through no fault of yours
- You lawfully obtain from a third party with rights to disclose
- Is generally known

Confidential obligations

You agree to:

- Use confidential information only for Company-related purposes
- Disclose only to those with a legitimate need -to-know
- Keep information secure and confidential
- Notify the Company immediately of any unauthorised disclosure and assist in mitigating it
- Not copy information except as reasonably necessary

Obligations continue indefinitely, unless information enters the public domain lawfully.

Security

You must maintain effective security to prevent unauthorised access, use, loss, or disclosure of confidential information.

Acknowledgement and Indemnity

- Breaches may cause irreparable harm, Company may seek injunctive relief
- This agreement supplements any common law or statutory duty of confidentiality
- You indemnify the Company of any losses arising from a breach of this agreement

Intellectual Property

This agreement does not transfer any intellectual property rights; all intellectual property remains the property of the Company.

Return or Destruction of Information

Upon termination of this agreement or request, you must:

- Return all confidential information; or
- Destroy all copies and certify destruction to the Company

Post-termination

Confidentiality obligations survive termination of engagement.

General

- This agreement supersedes prior arrangements on confidentiality
- Changes must be in writing and signed by both parties

Executed as an Agreement

Signed by Contractor

Signature: _____

Full Name: _____

Signed by Footprints Community Limited

Signature: _____

Full name: _____

Position: _____

Revision history

Version no	Date commenced	Change description	Review date	Policy owner		Authorised by (CEO or Board)
				Position title	Functional Area	
1	9 June 2026	• Initial version (policy only) replacing previous Privacy and Confidentiality policy and procedure • Updated confidentiality form (Appendix A)	9 June 2028	General Manager Compliance and Reporting	Compliance and Reporting	Board