Privacy, Client and Employment Records Policy

Connect: Inner West Community Transport Group (Connect) is committed to protecting and upholding the right to privacy of all clients, staff, volunteers, Directors, contractors, and representatives of agencies with whom it engages. Connect is committed to protecting and upholding our clients' right to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

This policy establishes how Connect collects, uses, stores, accesses, discloses and disposes of personal information and records.

As far as reasonably practicable, Connect will ensure that:

- It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel;
- Clients are provided with information about their rights regarding privacy;
- Clients and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature;
- All staff and Directors understand what is required in meeting these obligations; and
- It will adhere to all requirements imposed under the *Privacy Act 1988 (Cth),* including the requirements imposed by the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth),* to strengthen the protection of personal information.

This policy will apply to all records and personal information held by Connect, whether hard copy or electronic, including client, employment, Board, governance, and corporate records, along with personal information collected through interviews, consultation, research or service delivery.

Connect may vary, replace or rescind this policy from time to time.

Record of policy development		
Version	**Date approved**	**Date for review**
1	16 March 2026	March 2028

Responsibilities and delegations	
This policy applies to	Connect employees and Directors Clients and service users Job applicants Volunteers Contractors
Specific responsibilities	Board: • Policy approval and oversight; and • Determination of appeals relating to access decisions where required.

	General Manager (Privacy Contact Officer): • Overall responsibility for privacy compliance; • Decisions regarding access to information and disclosure; and • Handling privacy enquiries, complaints and data breaches. Employees, Volunteers and Contractors: • Compliance with this policy and related procedures; and • Protection of personal, sensitive and or confidential information accessed or obtained in the course of their role.
Policy approval	Board

Policy context – this policy relates to:	
Standards	Australian Privacy Principles (APP's) Aged Care Quality Standards
Legislation	Aged Care Act 2024 Privacy Act 1988 Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) Fair Work Act 2009
Contractual obligations	
Organisation policies	Confidentiality and Access to Information Policy Code of Ethics and Conduct
Forms, record keeping, other documents	TBD

Key Definitions

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive Information: A subset of Personal Information including health information and other information defined under privacy law.

Employment Records: Records of Personal Information relating to a current or former employee, including statutory required employment records.

Client Records: Records containing Personal or Sensitive Information about clients or service users.

Collection of Personal Information

Connect will only:

- collect information that is necessary for its lawful functions and activities;
- collect information by fair and lawful means;

- obtain consent where required;
- inform individuals why information is collected, how it will be used and disclosed, and how it will be protected; and
- allow individuals to remain anonymous or use a pseudonym where permitted by law.

Use and Disclosure of Personal Information

Personal information will only be used for:

- the primary purpose for which it is collected;
- a related secondary purpose for which it is collected;
- compliance with legal or regulatory obligations; or
- preventing a serious threat to health and safety, or life.

Personal and confidential information must not be disclosed for personal benefit or unauthorised purposes.

Client Records

Collection and Content

Client records may include personal, contact, health, service, preference and consent information necessary for service delivery and reporting obligations.

Storage and Security

Client records and stored on secure, password protected systems and/or in locked cabinets, with access restricted to authorised employees only.

Client Access and Correction

Clients have the right to:

- access their records;
- request correction of inaccurate information;
- withdraw or vary consent where applicable.

Requests for access will be considered within five (5) working days and managed by the General Manager.

Retention and Disposal

Client records are retained for seven (7) years after last service provision, or seven (7) years after a client turns eighteen (18) years of age. Records will be securely archived and destroyed when no longer required.

Employment Records

Prospective Employees

Connect may collect Personal Information from job applicants for recruitment purposes, including from third parties. Consent is required to retain unsuccessful applications for future roles.

Employee Access to Records

Employees and former employees are entitled to access statutory employment records in accordance with the Fair Work Act and Regulations. Access to non-statutory employment records is limited and subject to lawful exceptions.

Maintenance and Retention

Employment and taxation records are retained for a minimum of seven (7) years in accordance with

legislative requirements.

Disclosure

Employment records may be disclosed:

- for a relevant purpose;
- to related bodies corporate; and or
- where required by law or court order.

Board and Corporate Records

Board papers, minutes and corporate records containing sensitive or commercial information are confidential. Access is restricted to authorised employees and Directors, subject to approval by the General Manager or the Board.

Data Breaches

A data breach includes unauthorised access to, disclosure of, or loss of Personal Information. Where a notifiable data breach is likely to result in serious harm, Connect will notify the affected individuals and report the breach to the Office of the Australian Information Commissioner.

Complaints and Queries

Privacy enquiries or complaints should be directed to the General Manager. Complaints will be managed promptly and in accordance with legal requirements.

Breaches of this Policy

Breaches of this policy may result in disciplinary action, up to and including termination of employment, and may also result in legal or regulatory consequences.

End of document
