CONNECT:INNER WEST
Community Transport Group Inc.

Privacy

Connect Inner West Community Transport Group ('Connect') is committed to protecting and upholding the right to privacy of clients, staff, volunteers, Board members and representatives of agencies we deal with. In particular Connect is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

Connect requires staff, volunteers and Board members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

Connect is subject to the Privacy Act 1988. The organisation will follow the guidelines of the *Australian Privacy Principles* in its information management practices.

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, Board members and volunteers understand what is required in meeting these obligations.

This policy conforms to the *Federal Privacy Act (1988)* and *the Australian Privacy Principles* which govern the collection, use and storage of personal information.

(Note: The Federal Privacy Act applies to organisations with an annual turnover over $3m or organisations that are health service providers, operators of a residential tenancy database, a contractor that provides services under a Commonwealth contract, an organisation that is related to a larger organisation or one which trades in personal information.

Many funding contracts may require that funded organisations comply with the Australian Privacy Principles).

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

Record of policy development		
Version	**Date approved**	**Date for review**
4	21 February 2022	21 February 2025

Responsibilities and delegations	
This policy applies to	Staff, Volunteers, clients and NDIS clients
Specific responsibilities	General Manager, Operations Manager, Board
Policy approval	Board

Policy context – this policy relates to:	
Standards	NDIS Code of Conduct NDIS Practice Standards Aged Care Quality Standards
Legislation	Federal Privacy Act 1988 Privacy and Personal Information Act (1998), NSW
Contractual obligations	NDIS Commission TfNSW
Organisation policies	Client Records
Forms, record keeping, other documents	RouteMatch

Procedures

Dealing with personal information

In dealing with personal information, Connect staff will:

- ensure privacy for clients, staff, volunteers or Board members when they are being interviewed or discussing matters of a personal or sensitive nature
- only collect and store personal information that is necessary for the functioning of the organisation and its activities
- use fair and lawful ways to collect personal information
- collect personal information only by consent from an individual
- ensure that people know what sort of personal information is held, what purposes it is held it for and how it is collected, used, disclosed and who will have access to it
- ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves
- take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure
- destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.

Responsibilities for managing privacy

- All staff are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.
- The General Manager is responsible for content in Connect publications, communications and web site and must ensure the following:
  - appropriate consent is obtained for the inclusion of any personal information about any individual including Connect personnel
  - information being provided by other agencies or external individuals conforms to privacy principles
  - that the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website
- The General Manager is responsible for safeguarding personal information relating to Connect staff, Board members, volunteers, contractors and members.

The Privacy Contact Officer

The Privacy Contact Officer will be the General Manager and is responsible for:

- ensuring that all staff are familiar with the Privacy Policy and administrative procedures for handling personal information
- ensuring that clients and other relevant individuals are provided with information about their rights regarding privacy
- handling any queries or complaint about a privacy issue

Privacy information for clients

At the initial intake process conducted by the Intake Officer, clients will be advised:

- what information is being collected,
- why it is being collected
- how their privacy will be protected and their rights in relation to this information.
- that information will only be used internally to aid their support
- that information will not be shared with third parties unless required by law, there is a need to prevent a serious threat to the their health or safety, or if there is a need to report a serious crime
- they have the right to access and correct their personal information
- they will be contacted immediately if any breech occurs and how Connect is addressing the situation.

- of their right to withhold information without prejudice, advising this may result in not being able to provide services in full or part if we lack the information to do so efficiently and effectively
- that their consent can be revoked at any time by contacting Connect and making this intention known
- they have the right to access information provided, which can be corrected, updated or withdrawn at any time be contacting Connect.

Privacy for interviews and personal discussions

To ensure privacy for clients or staff when discussing sensitive or personal matters, the organisation will ensure all face-to-face private interviews and discussions will take place with the General Manager privately.

Participants in research projects

People being invited to participate in a research project must be:

- given a choice about participating or not
- given the right to withdraw at any time
- informed about the purpose of the research project, the information to be collected, and how information they provide will be used
- given copies of any subsequent publications

The collection of personal information will be limited to that which is required for the conduct of the project. Individual participants will not be identified.

Organisational participants in research projects will generally be identified in Connect's research, unless the nature of a particular project requires anonymity or an organisation specifically requests it.

Breach of Privacy

A data breach is an unauthorised access or disclosure of personal information, or loss of personal information.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee

- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Should a data breach occur which is considered 'harmful' Connect is required to contact affected individuals and also report the breach to the Office of the Australian Information Commissioner ('Commissioner').

An eligible, and reportable 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 access or disclosure is likely to occur)
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

End of document
