GENERAL

This policy outlines Connect2Group's expectations regarding protecting the privacy of information which the organisation collects, uses and maintains for the purpose of conducting its business.

Connect2Group is committed to ensuring that the collection and management of personal information is transparent, accountable and adherent to all relevant legislative requirements including the Australian Privacy Principles defined within the *Privacy Act 1988*.

SCOPE

Connect2Group requires that all staff (including casual staff and volunteers) and members of the Management Committee comply with this policy at all times in collecting and handling personal information in the course of their employment or engagement. Personal information may include staff information (including personnel records or files) and client information, as relevant.

COLLECTION OF PERSONAL INFORMATION

Connect2Group will only collect personal information that is necessary to facilitate administrative processes or to provide a service to a client. Personal information is information or an opinion that identifies or could identify a person, whether it is true or not and whether it is recorded in a material form or not.

It may also be necessary for Connect2Group to collect sensitive information to perform some services. Sensitive information may include information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation, criminal record, health or genetic information or biometric information.

Personal and/or sensitive information collected by Connect2Group may include name; date of birth; age; gender; nationality; personal and emergency contact details; taxation, banking or superannuation details; drivers licence details; education history and qualifications; previous or current employment information and details of reference checks; police checks and blue card / yellow card registration; health and medical information; forensic orders; financial management information from the Public Trustee.

Information is collected directly from an individual unless it is unreasonable or impracticable to do so. When information is collected from someone other than the individual, Connect2Group will take reasonable steps to ensure the individual is notified.

Information may be collected by telephone, in person at a Connect2Group site or event, through the use of services and through interviews, forms and questionnaires.

Any information given voluntarily that is not required by Connect2Group will be destroyed or de-identified.

Individuals have the option of remaining anonymous or using a pseudonym (fictitious name) when interacting with Connect2Group unless there is a legal requirement for individuals to identify themselves or where it is not possible to deliver a service to individuals who have not identified themselves.

In terms of client service, the information collected will be accurate and factual to enable staff to effectively plan for and evaluate client progress.

Collecting information will not intrude unreasonably on the client's personal affairs. Advice will be given to clients and/or their advocates about the purpose of information collection and conditions regarding release before these actions occur.

USE AND DISCLOSURE OF PERSONAL INFORMATION

Personal information will not be disclosed without obtaining prior written consent from the client or staff member, except where required or authorised by law. Personal information is not disclosed to overseas recipients.

Photos or news stories relating to an individual will not be released without the prior written consent of the person.

The decision to collect and disclose information is based on the best interests of the individual.

Staff will recognise and respect the client's role in controlling what information is revealed and recorded. Only information relevant to the support requirements for the client will be maintained.

If the client does not have the capacity to make an informed decision regarding the disclosure of information, they will be given the opportunity to gain support from an advocate.

Sensitive information will not be released if it is judged by the Executive General Manager or General Manager of the Division to be of a damaging or detrimental nature. Reasons for this decision will be noted in the file notes.

Access to personal information held in client files is restricted to:

- The person or a person's guardian or administrator who has authority for the relevant area; for example, a person's administrator can access financial records
- Support staff (including casual staff) who need it to support the person
- Professionals employed to provide services to people living in residential services such as health professionals who need to access or record information
- People with legal authority to access files.

Connect2Group will take reasonable steps to ensure individuals are informed beforehand of situations where the law allows or requires information to be given to other parties.

Consent is not required if information is:

- Necessary to prevent or lessen a serious threat to the life or health of the client or a member of the public
- Subject to a subpoena
- Reasonably necessary for the enforcement of the law or for the protection of public money
- Used for the purpose for which it is obtained. For example, a record of the client's seizures may be required by the doctor managing the client's epilepsy treatment.

WHO HAS LEGAL AUTHORITY TO ACCESS PERSONAL INFORMATION?

Government Departments and their subsidiaries.

COMMUNITY VISITORS CAN:

- Require staff to answer questions and produce documents related to the support of clients including a document in the client's personal or medical file in accordance with the *Public Guardian Act 2014* (QLD)
- Inspect and take extracts from or make copies of relevant documents
- Talk in private with clients or staff.

THE SENIOR PRACTITIONER CAN:

- Inspect and copy any document relating to any person they believe may be subject to restrictive intervention or compulsory treatment
- Ask any questions about the person or their support.

WORKCOVER AUTHORITY INSPECTORS CAN:

- Request any information they require to perform their role, which may include components of people's files or health records. These requests must be referred to the Executive General Manager.

If information is used for direct marketing in accordance with the *Privacy Act 1988*, individuals can request not to receive further material from Connect2Group.

SECURITY OF PERSONAL INFORMATION

Personal information is stored in both paper and electronic formats in a manner that reasonably protects it from misuse, interference and loss and from unauthorised access, modification or disclosure.

Connect2Group is required to archive information in accordance with the Archiving, Retention and Disposal Procedure. Information is stored in paper and electronic formats.

When information is no longer required or the maximum retention period has been reached, Connect2Group will take reasonable steps to destroy the information or ensure that it is de-identified.

ACCESS TO PERSONAL INFORMATION

An individual has the right to access the personal information Connect2Group holds about them at any time and to update and/or correct it, unless one of the exceptions under the *Privacy Act 1988* applies (e.g. giving access would be unlawful or denying access is required or authorised by law).

For instances where an exception applies, the individual will be notified in writing of the reasons for refusal to give access and the process of lodging a complaint about the refusal.

If an individual wishes to access their personal information, they should approach the relevant Executive General Manager or General Manager.

A third party, whether family or not, may not access or be given personal information without the express approval of the client. In a case where a client cannot give informed consent, a Court-appointed guardian or administrator may access such information.

If necessary, Connect2Group will request a client advocate to speak to the client to try to determine their wishes. Connect2Group will provide or explain all information in a way that is understandable by the client or the informed decision maker.

MAINTAINING THE QUALITY OF PERSONAL INFORMATION

Connect2Group will take all reasonable steps to make sure that the client's personal information is accurate, complete, up-to-date, relevant and not misleading. It is important that a client or their agent advise us at the earliest opportunity of any significant changes to personal information so that our records can be updated.

Where information has been disclosed to a third party in accordance with this policy, Connect2Group will take reasonable steps to notify the third party of updated information unless it is impracticable or unlawful to do so.

If a staff member or coordinator becomes aware of some significant change in a client's circumstances, they should encourage the client to speak to the Executive General Manager or General Manager to have that information updated.

BREACHES TO PRIVACY & CONFIDENTIALITY

The Executive General Manager or General Manager may initiate disciplinary action and/or legal action against any person who contravenes this policy.

Any client who suspects a breach of their privacy has occurred can lodge a complaint through the Connect2Group Complaints Management Process. The External Complaints Management Policy and Complaints Brochure are available on the Connect2Group website. Connect2Group is committed to resolving complaints within a reasonable timeframe.