POLICY STATEMENT

Connect2Group respects the privacy of all people, including participants accessing the organisation's services and supports, employees, volunteers, Management Committee members, contractors and business partners. Connect2Group is committed to safeguarding personal information held in accordance with state and commonwealth legislation and associated rules and regulations as may apply.

SCOPE

This policy has application to all Management Committee members, employees, volunteers and contractors employed or engaged by Connect2Group

POLICY OUTLINE

COLLECTION OF PERSONAL INFORMATION

Connect2Group will only collect and release personal information with the written consent of the participant or individual involved, except in specified circumstances required or permitted by law, or in circumstances where there is an emergency and information may be required to preserve or maintain life.

Connect2Group will only collect personal information that is necessary, or required, to facilitate administrative processes or to provide a service to a participant. 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.

The personal information that Connect2Group may request from a person will depend on the type of relationship the person has with Connect2Group – for example whether the person is a participant accessing supports from Connect2Group, is an employee, volunteer or other stakeholder.

Personal and/or sensitive information collected by Connect2Group from individuals 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.

Personal information collected from participants may include: name, date of birth, age, gender, nationality, personal and emergency contact details, details of disability or health-related issues, medial history information, medications, forensic orders and financial management information from the Public Trustee. Clients of Employment Division may also be asked for information on work history, referees, police checks, Centrelink information and other details required to establish eligibility for services. Information is collected directly from an individual unless it is unreasonable or impracticable to do so. Where a person is not able to provide this information, Connect2Group may collect the information from another person who has legal responsibility for the person or who acts as a recognised representative/nominee for the person.

Connect2Group only collects personal information for purposes directly related to our business, such as:

- The provision of supports;
- Meeting the requirements of Government agencies, for example the National Disability Insurance Agency (NDIA) and the Department of Social Services (DSS);
- Operating our business.

In terms of participant supports, the information collected will be accurate and factual to enable employees to effectively determine eligibility, plan for and evaluate participant progress.

Collecting information will not intrude unreasonably on an individual's personal affairs. Advice will be given to participants and / or their representatives about the purpose of information collection and conditions regarding release before these actions occur. Participants are informed that Connect2Group will report any data breaches, whether actual or suspected, to them and to the Office

of the Privacy Commissioner. Participants are also provided with information on how to complain directly to the Commissioner regarding data breaches.

USE AND DISCLOSURE OF PERSONAL INFORMATION

Personal information will not be disclosed without obtaining prior written consent from a participant or employee, except where required or authorised by law.

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

Employees will recognise and respect the participant's role in choice and control over what information is revealed and recorded. Only information relevant to support requirements for the participant will be maintained.

Sensitive information may not be released if it is judged by the Chief Executive Officer 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 participant files is restricted to:

- The participant or their guardian or representative who has authority for the relevant area; (any identifying information of any person other than the participant concerned is to be deidentified)
- Support employees (including casual employees) who need it to support the person – such information will be limited only to information required to provide supports as outlined in the participant's NDIS Plan and Person-Centred Plan. It may also include critical information needed to provide safe supports, including medical information, details of medication, positive behavior support plans and details

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.

Community Visitors Can

- Require employees 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 employees.

THE SENIOR PRACTITIONER CAN

- Inspect and copy any document relating to any person subject to restrictive intervention or compulsory treatment in accordance with the *Public Guardian Act 2014 (Qld)*;
- 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 in accordance with the *Work Health and Safety Act 2011 (Qld).* These requests must be referred to the Chief Executive Officer.

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 un-authorised access, modification or disclosure.

Connect2Group is required to archive information in accordance with the *GO410PR Archiving, Retention and Disposal Procedure.* Information can be stored in either paper and/or 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 Chief Executive Officer or General Manager.

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

MAINTAINING THE QUALITY OF PERSONAL INFORMATION

Connect2Group will take all reasonable steps to make sure that participants' 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 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 an employee becomes aware of some significant change in a participant's circumstances, they should encourage the client to speak to the Chief Executive Officer or General Managers to have that information updated.

BREACHES TO PRIVACY AND CONFIDENTIALITY

The Chief Executive Officer or General Managers may initiate disciplinary action and/or legal action against any person who contravenes this policy. Any participant who suspects a breach of their privacy has occurred can lodge a complaint through the Connect2Group Complaints Management Process *GO364 Complaints Management Policy.*

NOTIFICATION OF DATA BREACHES

A data breach occurs if:

(a) There is un-authorised access, un-authorised disclosure of, or loss of, personal information held by Connect2Group;
(b) The access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

REPORTING DATA BREACHES

The organisation must make a Notification to the Office of the Privacy Commissioner if:

(a) It has reasonable grounds to believe that a data breach has occurred;
(b) It is directed to do by the Commissioner.

ASSOCIATED LEGISLATION

Legislative and Regulatory Authority for this Policy includes but is not limited to:

- The Information Privacy Act 2009 (Qld)
- The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- The National Disability Insurance Scheme Act 2013
- Supporting Rules, Regulation and Guidelines of the National Disability Insurance Agency (NDIA) and the NDIS Quality and Safeguards Commission
- The National Standards for Disability Services
- Freedom of Information Act 1982 (Cth)

Linked Documents to this Policy include but are not limited to

- ***CC372PO Client Rights and Responsibilities Policy***
- ***GO411PR Privacy And Confidentiality Procedure***
- ***GO410PR Archiving, Retention and Disposal Procedure***
- ***GO1139PO IT Security Policy & Principles***