Privacy and confidentiality

Context

This policy ensures that You Connect protect and handle personal information in accordance with the NDIS and relevant privacy legislation. We acknowledge an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered in order to provide a safe working environment and a high standard of quality.

The information we collect is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

This policy applies to all personal information, including sensitive personal information, used and held by the organisation for participants and employees.

Applicability

When
▪ applies to all personal information and sensitive personal information including the personal information of employees and participants ▪ applies to all company confidential information - that is any information not publicly available

Who
▪ applies to all representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

What is personal information?

Personal information includes (regardless of its accuracy):

- name
- address
- phone number
- email address
- date of birth
- recorded opinions or notes about someone
- any other information that could be used to identify someone.

What is sensitive personal information?

Sensitive personal information can include personal information that is normally private such as:

- health information
- ethnicity
- political opinions

- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexuality
- criminal record
- biometric information (such as finger prints).

What is a data breach?

A data breach is a type of security incident where personal, sensitive or confidential information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen or used by an unauthorised person or parties. A data breach where people affected by the data breach are at risk of serious harm as a result, is reportable to the Office of the Australian Information Commissioner.

Supporting Policy Directives

Privacy and confidentiality guidelines

- all confidential records, files and other documents including extra copies will remain the property of You Connect and must be returned on termination of employment
- all staff must sign the Workplace Confidentiality Agreement during the induction process
- employees must not disclose confidential information or make public statements concerning You Connect to the media
- we are fully committed to complying with the privacy requirements of the Privacy Act, the Australian Privacy Principles and for Privacy Amendment (Notifiable Data Breaches) as required by organisations providing disability services
- we are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework and relevant state or territory requirements
- we provide all individuals with access to information about the privacy of their personal information
- individuals have the right to request access to their personal records by requesting this with their contact person
- where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language, and nationality
- employees must not share personnel files, client information, office documents or any information relating to clients with any unauthorised persons unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued)
- participants have the option of being involved in external NDIS audits if they wish.

Security of information

- we take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.
- personal information is accessible to the participant and is able for use by relevant workers
- security for personal information includes password protection for IT systems, locked filing cabinets and physical access restrictions with only authorised personnel permitted access
- personal information no longer required is securely destroyed or de-identified.

Data breaches

- we will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only be relevant workers
- if we know or suspect your personal information has been accessed by unauthorised parties, and we think this could cause you harm, we will take reasonable steps to reduce the chance of harm and advise you of the breach, and if necessary the Office of the Australian Information Commissioner.

Breach of privacy and confidentiality

- a breach of privacy and confidentiality is an incident - follow the Manage incident process to resolve
- a breach of privacy and confidentiality may require an investigation
- an intentional breach of privacy and confidentiality will result in disciplinary action up to and including termination of employment.

Staff responsibilities

All employees and managers must ensure that:

- safe information practices are implemented within the workplace and that all employees are educated on this policy
- confidential files are not displayed in plain sight, and stored in an appropriate locked place when not being used by staff and that all confidential information is not to be discussed with any persons outside of all You Connect sties without prior approval of general managers of the CEO
- Unneeded files are archived or destroyed appropriately
- any missing files or information is immediately reported to general managers or the CEO
- breach of this policy is reported to management and acted upon immediately.

Whistleblowers

Any employee/volunteer/contractor that has reasonable grounds for suspecting wrongdoing is encourages to raise any concerns with their immediate manager through normal reporting channels, who will then notify HR and/or the CEO.

Grievance Procedure

This policy is concerned with disclosure of information in the public interest, and must not be used for trivial or frivolous matters and does not replace the Internal complaint procedure for matters affect employment.

Whistleblower confidentiality

If a person makes a report of alleged or suspected wrongdoing under this policy, You Connect will endeavour to protect that person's identity from disclosure. This may not occur if confidentiality is not a practical option.

False reporting by a claimed whistleblower

Where it is shown a false report of wrongdoing under the guise of whistleblowing has been made, that conduct will be considered a serious matter and the person may be subject to disciplinary action including dismissal.

Investigation of the report

All reports of alleged or suspected wrongdoing made under this policy will be properly assessed and if appropriate, independently investigated with the objective of locating evidence that either substantiates or refutes the claims made by the whistleblower.