Privacy Policy

Policy area	Information Management and Privacy
Document type	Policy
Applicable to	Complete Support & Co
Version	1.1
Date approved	18th March 2026
Approved by	Director
Next review date	18th March 2027
Related policies	Information Management Policy Governance Policy Risk Management Policy Incident Management Policy Consent Policy Client Advocacy Policy Duty of Care Policy Human Resources Management Policy Surveillance Technology Policy
Authority	Privacy Act 1988 Australian Privacy Principles Privacy Amendment (Notifiable Data Breaches) Act 2017 NDIS Act 2013 NDIS Practice Standards and Quality Indicators UN Convention on the Rights of Persons with Disabilities UN Convention on the Rights of the Child NDIS Code of Conduct Aged Care Act 1997 Aged Care Quality and Safety Standards Aged Care Code of Conduct

PURPOSE

The purpose of this policy is to explain our organisation's commitment and approach to protecting individuals' personal and sensitive information and privacy.

SCOPE

This policy applies to all our workers (employees, contractors and volunteers).

DEFINITIONS

Term	Definition
Personal Information	This is defined in the Privacy Act 1988 as follows:

	'Information or an opinion about an identified individual, or an individual who is reasonably identifiable: a) whether the information or opinion is true or not; b) whether the information or opinion is recorded in a material form or not.' It includes: ● **information about a person's private or family life** (e.g. name, signature, email address, phone number, date of birth, medical records, bank account details and employment details); ● **information about a person's working habits and practices** (e.g. work address, contact details, salary, job title); ● **commentary or opinion about the person** (e.g. written comments by a referee, trustee, journalist). Information that does not identify an individual or information that is not 'about' an identified individual is not included in 'personal information'.
Sensitive Information	This is a type of 'personal information' and includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record. Health information is also classified as 'sensitive information'.

CONTEXT

Our organisation is committed to protecting clients' and workers' personal and sensitive information. We will:

- implement compliant and transparent processes for collecting, using, disclosing and storing personal and sensitive information;
- maintain an effective information management system; and
- uphold clients' and workers' right to privacy and confidentiality.

POLICY STATEMENT

1. Compliance

- We will comply with all applicable federal and state/territory legislation, regulations, standards and principles in relation to the collection, use, disclosure, retention and storage of personal and sensitive information.
- We will conduct regular audits to ensure the integrity of our information management and privacy protection processes.

2. Communication and Consent

- We will discuss with the client or family/alternate decision-maker/advocate their rights in relation to privacy and confidentiality in a language, mode and method they are most likely to understand.
- We will explain to the client and/or family/alternate decision-maker/advocate, in a language, mode and method they are most likely to understand, the types of information we collect from them, why we collect it and how we use and store their information.
- We will obtain written consent from the client and/or family/alternate decision-maker/advocate before disclosing and sharing personal information with third parties.
- We will ensure the client is aware of their right to change or withdraw their consent in relation to their personal information at any time and support them to do so, if requested.

3. Access

- We will provide the client and/or family/alternate decision-maker/advocate with access to the client's personal information and assist them to make changes to their personal information, if requested.
- We will discuss with the client and/or family/alternate decision-maker/advocate, in a language, mode and method they are most likely to understand, circumstances when their personal information may be accessed by authorised personnel (e.g. law enforcement, official investigation, public health order).
- We will take reasonable measures to ensure personal information is stored safely and securely and protected against misuse, loss, unauthorised access or interference.

4. Complaints

- We will discuss with the client their right to lodge a complaint, both internally and externally, if they have a concern about their personal and sensitive information and privacy and support them to do so if requested.
- We will discuss with the client their right to engage an advocate to speak on their behalf and raise any privacy or confidentiality concerns they have.

5. Information and Record-keeping

- We will ensure information and records are accurate and up to date.

- We will ensure the client has provided us with all required written consents.
- We will store the information securely to ensure privacy, dignity and confidentiality and make sure it is accessible to the client and only other stakeholders authorised to access it.

6. Worker Training and Supervision

- We will maintain a skilled and trained workforce which is aware of clients' human and legal rights and in particular, the right to privacy and dignity.
- We will maintain processes to adequately monitor and supervise workers.

SUPPORTING DOCUMENTS

Related procedures and forms include:

- Management of Data Breach Procedure
- Risk Management Procedure
- Incident Management Procedure
- Reportable Incident Management Procedure
- Client Advocacy Procedure
- Surveillance Technology Procedure
- Privacy Statement
- Easy Read – Privacy and Personal Information
- Privacy and Confidentiality Agreement
- Participant Information Consent Form
- Third Party Information Release Consent Form
- Data Breach Process Form
- Document Control Register

RESPONSIBILITIES

Operations Manager is responsible for:

- maintaining this policy, its related procedures and associated documents;
- ensuring the policy is effectively implemented across the service;
- monitoring workers compliance with the requirements of this policy; and
- ensuring training and information is provided to workers to carry out this policy.

All workers are responsible for complying with the requirements of this policy.

COMPLIANCE

Deliberate breaches of this policy will be dealt with under our misconduct provisions, as stated in the Code of Conduct Agreement.