Information Management Policy

Policy area	Information Management and Privacy
Document type	Policy
Applicable to	Beyondlimits Care & Support Services
Version	001
Date approved	19/08/2024
Approved by	Managing Director
Next review date	Every 12 Months
Related policies	Privacy Policy Consent Policy Risk Management Policy Governance Policy Emergency and Disaster Management Policy Human Resources Management Policy Work Health and Safety Management Client Health and Wellbeing Policy Incident Management Policy Transition of Care Between Different Environments Policy Continuous Improvement and Quality Management Policy Client Feedback and Complaints Management Policy Support Planning Policy Service Access and Exit Policy Service Delivery Policy
Authority	Privacy Act 1988 Australian Privacy Principles Privacy Amendment (Notifiable Data Breaches) Act 2017 Australian state and territory privacy legislation NDIS Act 2013 NDIS Practice Standards and Quality Indicators UN Convention of the Rights of Persons with Disabilities 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 information management.

SCOPE

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

DEFINITIONS

Term	Definition
Official Records	These include: ● **service delivery records** (e.g. client files, case/progress notes, support plans, service agreements, health reports, assessments, incident reports); ● **business activity records** (e.g. written records on business support, project management, finances, quality and compliance); ● **human resource management records** (e.g. worker files, incident reports, timesheets, worker training analysis, recruitment and selection criteria, position descriptions). Official records are records which would 'stand up in court' and include email correspondence, work diaries and notebooks if they contain details of client or business interactions and records of decisions or actions.
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 recognises the importance of maintaining an effective and compliant information management system for safe and quality client service delivery and business activity operations.

POLICY STATEMENT

1. Compliance

- We will maintain an information management system and processes that support compliance with 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 ensure our information management system is proportionate to the size and scale of our organisation and the scope and complexity of services and supports provided.

2. Creation and Maintenance of Information and Records

- We will create and maintain accurate and complete information and records.
- We will maintain processes for document version control and ensure information from different sources is integrated, consistent and up to date.
- We will maintain all required written client and worker consents and agreements.

3. Consent

- We will seek informed consent from the client to collect, use, store and disclose their personal information (including assessments) to other parties.
- We will ensure the client understands their right to change or withdraw their consent at any time and assist them to do this if requested.

4. Access, Distribution, Storage and Retention of Information and Records

- We will provide the client with access to their personal information and assist them to correct or change their information, if requested.
- We will provide access to client information to the client's family/alternate decision-maker/advocate, with the client's consent.
- We will maintain processes to ensure client information is, with the client's consent, communicated within the organisation to authorised workers and with others outside the organisation where responsibility for care is shared (e.g. client transitioning to another environment such as hospital, hospice, respite or residential facility).
- We will provide worker and client access to the right information at the right time to ensure safe and quality service provision.
- 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 (law enforcement, official investigation, public health order).

- We will maintain policies, procedures, forms and templates that are current, regularly reviewed, informed by contemporary evidence-based practices, and are understood and accessible by workers.
- We will store personal information securely and take reasonable steps to protect it against misuse, loss, unauthorised access or interference.
- We will retain records in accordance with legislative requirements. This includes disposal freezes and retention notices declared by bodies such as the National Archives of Australia and/or equivalent state/territory bodies that are in force from time to time.

5. Security of Information and Records

- We will maintain processes to back up online data weekly and conduct periodic testing of the backed-up data to check system integrity.
- We will store hard copy records <offsite using an engaged archival company in an onsite locked filing cabinet>.
- We will maintain secure log-in credential processes to ensure that only current authorised workers have access to relevant online files, folders, drives and intranet sites.
- We will implement a business continuity plan to ensure the security of information and records during and after an emergency or disaster event.
- We will manage and report notifiable data breaches in accordance with legislative requirements and the Managing Data Breaches Procedure.

6. Complaints

- We will discuss with the client their right to lodge a complaint, both internally in our organisation and externally to a regulator, if they have a concern about their personal and sensitive information and privacy and support them to do so if requested.

7. Reviewing and Monitoring Processes

- We will conduct regular audits to ensure the integrity of our information management and privacy protection processes.
- We will review and improve the effectiveness of our information management system.

- We will maintain a Complaints Register and a Continuous Improvement Register with details, actions and outcomes of complaints and suggested improvements in relation to information management.

8. Worker Training and Supervision

- We will maintain a skilled and trained workforce which is aware of the importance of accurate and complete record-keeping, security of personal and business information and data and human and legal rights in relation to privacy.
- We will maintain processes to adequately monitor and supervise workers.

SUPPORTING DOCUMENTS

Related procedures and forms include:

- Privacy Statement
- Privacy Statement – Easy Read
- Privacy and Confidentiality Agreement
- Participant Information Consent Form
- Third Party Information Release Consent Form
- Data Breach Process Form
- Privacy Statement
- Document Control Register
- Management of Data Breach Procedure
- Risk Management Procedure
- Emergency and Disaster Management Procedure
- Transition of Care Between Different Environments Procedure
- Client Feedback and Complaints Management Procedure
- Support Planning Procedure
- Service Access and Exit Procedure
- Service Delivery Procedure
- Continuous Improvement and Quality Management Procedure

RESPONSIBILITIES

Managing Director 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.