Information Management Policy and Procedure

1.0 PURPOSE:

Back2You Therapy is committed to implementing and maintaining robust communication processes and information management systems. All information systems and practices are carefully aligned with legislative and regulatory compliance requirements, as well as organisational standards. Continuous improvement is a priority to ensure compliance and excellence in information management.

2.0 SCOPE:

It is Back2You Therapy's policy that records are established for all participants, Support at Home clients receiving aged care services, staff, volunteers and contractors upon entry to the service and maintained for the duration of their engagement with the company. This policy applies to information collected, used, stored, disclosed, accessed, corrected, archived and destroyed in relation to NDIS supports and aged care services delivered in the home.

3.0 POLICY:

- The company maintains effective information management systems to ensure privacy and confidentiality for all stakeholders.
- The company complies with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), the NDIS Information Rules where applicable, and relevant aged care information management and privacy obligations for Support at Home clients. This covers the collection, use, storage, protection, access, correction and disclosure of personal, health, NDIS and aged care information. NDIS and aged care-related information is managed according to these requirements, including:
    - Only collecting information necessary for the provision, coordination, review and funding of supports and services, including Support at Home aged care services, and as permitted by law

- Obtaining informed consent, or where relevant consent from an authorised representative, for the collection, use, storage and disclosure of NDIS or aged care information; recording consent within participant or client files
- Using and disclosing NDIS or aged care information strictly for its intended and authorised purposes or as required or authorised by law, including for reportable incidents, serious risks to health, safety or wellbeing, complaints, quality and safety obligations, or other statutory requirements
- Taking all reasonable steps to protect information from misuse, interference, loss or unauthorised access, modification or disclosure, using proper access controls, secure physical storage and staff training
- Maintaining an accurate record of authorised disclosures, ensuring all disclosures are compliant with applicable NDIS, aged care and privacy requirements
- Responding to requests for access to or correction of NDIS or aged care information in accordance with the Privacy Act 1988 (Cth), NDIS Information Rules where applicable, and aged care requirements.
- For Support at Home clients, records must support safe, person-centred aged care by ensuring information is accurate, current, confidential, accessible to the client and their authorised supporters where appropriate, and available to workers and health professionals who need it to deliver quality care.

- The company adheres to the Australian Privacy Principles (APP) as outlined below:
  - Consideration of personal information privacy
    - APP 1 – Open and transparent management of personal information
    - APP 2 – Anonymity and pseudonymity
  - Collection of personal information
    - APP 3 – Collection of solicited personal information
    - APP 4 – Dealing with unsolicited personal information
    - APP 5 – Notification of the collection of personal information
  - Dealing with personal information
    - APP 6 – Use or disclosure of personal information
    - APP 7 – Direct marketing

        - APP 8 – Cross-border disclosure of personal information
        - APP 9 – Adoption, use or disclosure of government-related identifiers
    - The integrity of personal information
        - APP 10 – Quality of personal information
        - APP 11 – Security of personal information
    - Access to and correction of personal information
        - APP 12 – Access to personal information
        - APP 13 – Correction of personal information
- Policies and procedures are stored in read-only format within the Policies and Procedures folder on the shared drive.
- The company, with support from the Director and relevant staff, is responsible for keeping this information up to date.
- The company encourages the active involvement of all staff to ensure policies and procedures remain practical, current and reflective of best practice.
- A copy of each organisational form is maintained in the shared drive.
- All staff may access policies and procedures in electronic formats on shared drive.
- Reviews of policies and procedures occur at a minimum of every three (3) years.
- Superseded documents are deleted from the Policies and Procedures folder and are electronically archived by the Director or their delegate.

4.0 PROCEDURE:

4.1 The company information management system

4.1.1 Participant documentation procedure

- Participants and Support at Home clients are informed about:
    - The reasons for collecting personal information
    - How their information will be used and disclosed
    - How their information will be used and disclosed, including sharing information with authorised supporters, aged care workers, registered health

practitioners, allied health professionals, allied health assistants or other providers involved in their care where consent or lawful authority applies
    - Information management practices
    - Relevant government requirements, including opt-out options
    - Their rights under applicable aged care arrangements, including dignity, respect, privacy, choice, and involvement in decisions about how information is collected and shared
    - How they may access their information
    - How to request changes to their information
- Participants are also made aware of their right to withdraw or amend consent at any time. The process for making such a request is clearly set out, including:
    - How to notify the organisation (verbally or in writing to the Director or their delegate)
    - Expected processing timeframes (requests are recorded upon receipt and, where feasible, processed within five business days)
    - Any implications that withdrawing or amending consent may have on service provision, which are to be explained to the participant
    - Documenting all withdrawals or amendments in the participant's file and the organisation's electronic system
- The privacy and confidentiality of participant records are strictly upheld.
- All staff and volunteers who provide, direct or coordinate supports are required to document their activities.
- Participant and Support at Home client files are to accurately reflect service and support delivery, and typically include:
    - Personal and contact details
    - Referral information
    - Assessments
    - Support plans and goals
    - Personal emergency preparation plans
    - Reviews of support
    - Service delivery and response details

  - Aged care assessment, care plan, service delivery, clinical and allied health information relevant to Support at Home services
- Original documentation is filed centrally for each participant.
- Updates regarding the participant's situation, including changes to risk or health status, are documented in their notes.
- Staff receive training in documentation and record-keeping relevant to their roles.
- Every staff member is expected to understand individual requirements, goals, and strategies, with reference to support and emergency plans.
- Staff must not document information on behalf of others.
- Regular audits of participant records are conducted to ensure their completeness and compliance with quality standards.
- All records are stored securely, with access granted only to authorised personnel.
- Service agreements are maintained in accordance with NDIA guidelines and are accessible according to the participant's communication needs.
- Documentation by brokerage agencies regarding their activities is required under service agreements.
- Notes concerning a participant must be entered promptly, with accuracy and factual detail.
- Information collected is used solely for the purpose it was intended.
- Participants are advised that de-identified data may be used for planning, evaluation or promotion, without revealing their identity.
- Participants, their families and advocates have the right to access their collected personal information, with staff providing appropriate support for access as needed.
- For Support at Home clients, information must be kept accurate, current and integrated from relevant sources so workers and professionals have access to the right information at the right time to deliver safe and quality aged care services in the home.

4.1.2 Entering the company's service

Upon a participant joining the service, informed consent is documented using the approved Service Agreement before any data collection occurs. Initial information is then collected via Referral Form, limited to what is necessary for assessing and managing support needs.

A central participant file is created to store all service-related information and communications. Each participant may be allocated a unique identifier for record-keeping.

The participant's file includes only material directly relevant to support and service management, such as:

- Signed service agreements
- Assessment and health reports
- Risk assessments
- Communication notes
- Consent records
- Emergency plans
- Complaints and feedback

4.1.3 Ongoing documentation procedures

Ongoing requirements include:

- Maintaining up-to-date participant records in the electronic management system
- Using only authorised forms or tools for service documentation
- Regularly revising documents during reviews or in response to emergencies
- Ensuring external professionals involved in care also provide adequate updates regarding participant wellbeing

Records maintained include:

- Outcomes of assessments or reassessments
- Updates to support plans reflecting new goals or preferences
- Critical incidents or significant changes in wellbeing
- Responses to emergencies or disasters
- All relevant discussions with participants, families, advocates or external providers
- Activities and notes related to service admission or exit

4.1.4 Setting up and maintaining files for participants

Staff are responsible for encouraging the accuracy and currency of participant files by promptly documenting events and significant issues as they arise.

Non-current materials (no longer relevant to current services) are transferred to archival files for secure storage. Regular audits, carried out by the Director, confirm:

- Documentation is current and complies with requirements
- Appropriate forms are in use
- Non-current information is managed and archived appropriately
- File notes are accurate, factual and recorded in sequence

Upon participant exit, both current and archival files are stored securely—for example, in a locked area or password-protected electronic folder under company control.

4.1.5 Participant file formats

Participant files are established as:

- Secure electronic files with password protection

Archival files may be stored in lever-arch folders, archive boxes or on approved electronic platforms. They are organised for easy retrieval, using chronological order and consecutive page numbering.

4.1.6 Security of files and participant information

Electronic files are password protected to ensure confidentiality. Files may be removed from the service only by authorised staff for direct support purposes, or if relocated with permission from the Director.

Non-current files are only removed for transfer to secure archival storage, with appropriate authorisation. No confidential documents or data may be copied, shared or communicated without express approval. This includes copying to other devices, cloud platforms or unauthorised persons.

4.1.7 Communication/file notes for participants

- Notes must record:
    - Date and time of entry
    - Time when the described event occurred
    - Factual and clear nature of the event

- Signature, printed surname (in brackets), and position of the person making the entry

- All relevant details must be documented promptly each workday, whether or not significant events occurred.
- Entry of notes on behalf of another staff member is only permitted if the actual staff member reviews and signs off at the earliest opportunity.
- Participants should be informed as necessary about what is recorded in their notes.

4.1.8 Working from home

Staff working remotely are required to sign a Privacy and Confidentiality Agreement, complying with requirements including:

- Restricting access to records to the staff member only
- Use of a firewall on computers
- Uploading locally stored information to the server each day
- Recording work hours and sharing status updates regularly with supervisors

4.1.9 Access to participants' files

Participants and guardians may request access to their records. The Director is responsible for approving and facilitating access, ensuring any release of records does not compromise the privacy of others.

Participant files belong to the company and, while they can be accessed as above, cannot be removed or transferred without written permission. All releases of files are properly recorded.

Where permitted by law (e.g. mandatory reporting, court orders), disclosure may proceed without consent, with documentation and Director review. Students may access records only with the participant's consent and sign confidentiality undertakings as required.

4.2 Staff records

Files are established in:

- Secure electronic formats with appropriate password protection

4.3 Minutes of meetings

Minutes are filed in an identifiable folder within the shared drive (e.g. 'Management Meetings'), consistently named by meeting type and date for clear reference.

4.4 Other administrative information

Staff are individually responsible for managing and filing routine administrative information in line with their roles. Administrative material, including funding and financial documents, are held securely in the Director's office, with electronic files password-protected.

4.5 Electronic information management

4.5.1 Data storage

- Company data is stored on a shared drive on the main server.
- Only the Director can add new folders to this drive.

4.5.2 Backup

- All computer data (including emails) is backed up nightly to a remote server.
- Backups are periodically tested for integrity and recoverability.

4.5.3 External programs

- No external programs or utilities are installed on any workstation without explicit permission from the Director.

4.5.4 Log-in credentials

- Log-in credentials are issued by the Director or delegate, ensuring secure, individualised access.

4.5.5 Email

- Sending and receiving personal emails is not permitted unless expressly approved.
- All emails must be filed in appropriate folders.
- Inappropriate or spam emails must be deleted immediately and never opened or actioned.

4.5.6 Internet access

- Internet use is strictly for work-related purposes.
- Monitoring is carried out through reporting, with regular oversight from the Director.
- Access to inappropriate websites is strictly prohibited.

4.5.7 IT Support

- Issues should be reported initially to the Director who will coordinate IT support as required.

4.5.8 Social media

- The use of social media is guided by the obligation to maintain privacy and confidentiality of all organisational and participant information.
- Staff are reminded not to share or discuss work-related information online and to consult the Director with any uncertainties.

4.6 Monitoring information management processes and systems

Routine audits are conducted as part of continuous improvement. Feedback from staff, participants and stakeholders is welcomed and used to enhance information management practices.

4.7 Archival and storage

Records are retained in line with the following minimum retention periods or as required by legislation or other regulatory obligations:

- Aboriginal and Torres Strait Islander participant information: Lifetime (permanent retention unless otherwise directed)
- General participant records: Seven years post last service contact (or to age 25 if the individual was a child at service time)
- Incident records: At least seven years after the incident date; longer if required
- Complaints: Minimum seven years from resolution or closure
- Restrictive practices: Minimum seven years from last application or as required

- Staff records: Seven years after employment ends; longer if required
- Financial records: Seven years
- Contracts and leases: Seven years after expiry/termination or as mandated
- Audits and management reviews: Minimum two years unless otherwise regulated

Archived files are organised for easy retrieval and stored in a way that minimises deterioration (out of direct sunlight, with protection from moisture, pests and fire risks).

Where additional retention is mandated (e.g. for taxation), the longer statutory period applies.

4.8 Destruction of records

Procedures for record destruction include:

- No records are to be destroyed before the minimum retention period has passed. Staff must verify and obtain appropriate approval from the Director (or delegate) prior to destruction.
- Routine notes and non-essential items (e.g. junk mail) may be recycled.
- Sensitive records scheduled for destruction must be shredded, securely disposed of off-site, or deleted to prevent recovery.
- All destruction is documented, recording record type, destruction date, method, and the person authorising or carrying it out. These records are retained for at least two years for audit purposes.

5.0 REFERENCES:

- Disability Discrimination Act 1992 (Commonwealth)
- Privacy Act 1988 (Commonwealth)
- Work Health and Safety Act 2011 (Commonwealth)
- NDIS Practice Standards and Quality Indicators 2021
- Aged Care Act 2024 (Commonwealth)
- Strengthened Aged Care Quality Standards, including Outcome 1.2 Dignity, Respect and Privacy and Outcome 2.7 Information Management

Attachment 1: Disposal and archiving of documents

Function or Activity	Description	Retention/ disposal action	Custody
Aboriginal and Torres Strait Island participant information	Documents relating to Aboriginal health	Lifetime	Office
Standard operational documents	Seven years after the person's last contact with the service		
Business information	Name Address Telephone number Compliance notices Financial records	Seven years	Office
Internal audits	Audit schedule Audit questions Audit reports	Two years	Office

Function or Activity	Description	Retention/ disposal action	Custody
Participant records	Name Address Telephone number Emergency Contact Application Complaints about non-delivery of services Incident Records Complaint Records BSP Records Service Agreement Personal Emergency Preparation Plan	Seven years If the participant is a child, records must be stored until the child turns 25.	Office
Contracts/leases	Properties	Seven years	Office
Corrective action	Corrective action Requests	Two years	Office
Financial	Audits Budgets Receipts Cheques Petty cash documents Other financial records	Seven years	Office

Function or Activity	Description	Retention/ disposal action	Custody
Management review	Minutes of meetings Agendas Monthly reports	Two years	Held on PCs according to the type of meeting