



Information Management Policy and Procedure in Easy English

Information Management Policy and Procedure

1.0 Purpose

This section tells you why we have this policy.

- We keep and manage information safely and correctly.
- We follow the law and NDIS rules when we handle information.
- We want your information to be private and secure.

2.0 Scope

This section tells you who this policy covers.

- This policy covers participants, staff, volunteers and contractors.
- We make a record for each person when they start using our service.

3.0 Policy

This section tells you the main rules we follow.

- We keep information private and confidential.
- We follow the Australian Privacy Principles (APP) and the NDIS Information Rules.
- We only collect information we need to support you.
- We only use information for the reason we collected it.
- We only share information when you agree or the law requires it.
- We will limit any lawful sharing to what is needed.
- Our policies are stored as read-only on the shared drive.
- DIRECTOR helps keep these policies up to date.
- All staff are encouraged to help improve the policies.
- All forms are kept in the Forms folder on the shared drive.

- Staff can access policies in paper or electronic form at the office.
- Policies are reviewed at least every three (3) years.
- Old policies are deleted and archived by DIRECTOR or a delegate.

4.0 Procedure

This section tells you how we handle information day to day.

4.1 The company information management system

4.1.1 Participant documentation procedure

This section tells you what we tell participants and how we keep records.

- We tell you why we collect your information and how we use it.
- We tell you how we keep it safe and how you can access it.
- We keep participant records confidential.
- Staff and volunteers who support you must write down what they do.
- We keep accurate notes about your services and supports.
- Files can include personal details, referrals, assessments, support plans, goals, emergency plans, reviews and service details.
- Original documents go in your central file.
- Changes to your health or risks must be recorded.
- All staff are trained in good record keeping.
- Only the person who did the work may make the notes.
- We audit participant records regularly for quality.
- Files are stored securely and only authorised people can see them.
- Service agreements match your NDIS plan and your communication needs.
- Brokerage workers must also record their work.
- Staff must write factual and timely notes.
- We may use non-identifying data for planning and promotion.

- You, your family or your advocate can ask to see your information. Staff will help you.

4.1.2 Entering the Company's service

This section tells you what we collect when you join our service.

- We use the Participant Intake Form to collect initial information.
- We only collect personal information we need to support you.
- We use an Assessment Report, Individual Risk Profile, Support Plan and Personal Emergency Preparation Plan.
- DIRECTOR will work with you, your advocate, family and other providers to make your Support Plan.
- We keep a participant file as the main record of your supports.
- Your file may have a unique identifier for record-keeping.
- Files only include material needed to manage your supports.

4.1.3 Ongoing documentation procedures

This section tells you how we keep records while you use our service.

- We keep records in our electronic participant system following its rules.
- Use only approved forms and tools to record information.
- Update documents at reviews and in emergencies.
- Other services and health professionals must provide records about their work with you.
- We record assessment results, plan changes, incidents, emergencies and important conversations.
- We record admission and exit activities and referrals.

4.1.4 Setting up and maintaining files for participants

This section tells you how we look after participant files.

- Staff must record important events as they happen.
- Non-current information is moved to an archive file.
- DIRECTOR audits files to make sure they are current and correct.

- Files are stored securely when someone leaves the service.

4.1.5 Participant file formats

This section tells you the types of files we use.

- Files may be paper in a folder or electronic with a password.
- Use the company's approved form formats.
- Archive files may be in boxes or electronic archives.
- Archive items should be in order and easy to find.

4.1.6 Security of files and participant information

This section tells you how we keep information safe.

- Hard copy files are kept in lockable storage.
- Only authorised staff can access participant files.
- If files cannot be kept at the service, DIRECTOR will arrange secure storage with the participant.
- Electronic files must be password protected.
- Staff can take files to another service (for example, a doctor) only when needed and authorised.
- Non-current files should not be removed unless moved to secure archive or with DIRECTOR permission.
- Do not photocopy or copy confidential records without DIRECTOR approval.
- Do not share confidential data with unauthorised people.

4.1.7 Transporting a participant's hard copy files

This section tells you what to do when paper files travel.

- Use a locked document container when moving paper files.
- The Company will provide a locked case if needed.

4.1.8 Communication/file notes for participants

This section tells you what to put in notes.

- Each note must have the date and time of entry.
- Record the time the event happened.
- Write the event in a factual and accurate way.
- Sign the note and print your surname and job title.
- Write notes when a significant event happens or each workday.
- Do not leave blank lines in notes.
- If you write notes for another staff member, they must sign their entry at the next shift.
- Participants can ask to see what is recorded about them.

4.1.9 Working from home

This section tells you the rules for working from home.

- Staff working from home must sign the Privacy and Confidentiality Agreement.
- Only the staff member can access work documents at home.
- The computer must have a firewall.
- Upload server files at the end of each day.
- Record start and finish times and send them to your supervisor.
- Report your work status at least weekly.

4.1.10 Access to participants' files

This section tells you how people can see files.

- Participants and guardians can ask to see their records.
- DIRECTOR controls and approves access to protect privacy.
- Files are the property of the Company. They cannot be taken away without permission from DIRECTOR.
- Copies given to others must be recorded and signed for.
- Students only access files with participant consent and must sign confidentiality agreements.

4.2 Staff records

This section tells you how we keep staff files.

- Staff files are kept in a locked filing cabinet in DIRECTOR's office.
- Only DIRECTOR can access these files.
- Staff files can be paper folders or electronic with password access.

4.3 Minutes of meetings

This section tells you how we keep meeting notes.

- Minutes are stored on the shared drive in a clear folder.
- Name minutes with the meeting title and date.

4.4 Other administrative information

This section tells you who looks after admin records.

- Staff keep general records as part of their job.
- Funding and financial files are in locked cabinets in DIRECTOR's office.
- Electronic admin files are password protected.

4.5 Electronic information management

4.5.1 Data storage

This section tells you where we store data.

- All data is stored on the server shared drive.
- Only DIRECTOR can add new folders to the shared drive.

4.5.2 Backup

This section tells you how we back up data.

- All computer data is backed up to a remote server every night.
- We test backups sometimes to make sure they work.

4.5.3 External programs

This section tells you about installing software.

- Do not install programs on work computers without DIRECTOR permission.

4.5.4 Log-in credentials

This section tells you who gives login details.

- DIRECTOR or their delegate assigns log-in details.

4.5.5 Email

This section tells you the rules for email.

- Staff should not use work email for personal messages unless approved by DIRECTOR.
- All work emails must be filed in the right folders.
- Delete pornographic or spam emails immediately. Do not open them.

4.5.6 Internet access

This section tells you the rules for internet use.

- Internet is for work only.
- DIRECTOR reviews internet use reports.
- Do not access pornographic sites.

4.5.7 IT Support

This section tells you how to get tech help.

- Contact DIRECTOR first for IT problems.
- DIRECTOR can arrange IT consultant help if needed.

4.5.8 Social media

This section tells you the rules for social media.

- Do not share confidential information about the Company or participants.
- Do not post work information without checking with DIRECTOR.
- Ask DIRECTOR if you are unsure about sharing anything online.

4.6 Monitoring information management processes and systems 🔍

This section tells you how we check our systems.

- We audit our information systems regularly.
- Staff, participants and others can give feedback to help us improve.

4.7 Archival and storage 📁

This section tells you how we keep old records.

- We keep archived records for the time the law or good practice says.
- Archived records are stored so they are easy to find.
- Keep paper archives away from sun, moisture, pests, dust and fire risk.

4.8 Destruction of records 🗑️

This section tells you how we destroy records.

- Junk mail and notes go in recycling.
- Confidential records are shredded or pulped securely.
- We delete electronic records from the network.

5.0 Related documents 📄

This section lists documents linked to this policy.

- All electronic and hard-copy documentation
- Complaints Register
- Service Agreement
- Privacy Statement - Website
- Participant Intake Form
- Participant Information Consent Form
- Personal Emergency Preparation Plan
- Support Plan
- Consent Policy and Procedure

6.0 References

This section lists laws and standards we follow.

- Disability Discrimination Act 1992 (Commonwealth)
- Privacy Act 1988 (Commonwealth)
- Work Health and Safety Act 2011 (Commonwealth)
- NDIS Practice Standards and Quality Indicators 2021

Attachment 1: Disposal and archiving of documents

This section tells you how long we keep different records.

- Aboriginal and Torres Strait Island participant information: keep for life. (Office custody)
- Standard operational documents: keep for seven years after last contact.
- Business information (name, address, phone, compliance, financials): keep seven years. (Office custody)
- Internal audits (schedule, questions, reports): keep two years. (Office custody)
- Participant records (contacts, emergency contact, applications, incidents, complaints, BSPs, service agreements, emergency plans): keep seven years after last contact. If the participant is a child, keep until they turn 25. (Office custody)
- Restrictive practice records: keep seven years. If the participant is a child, keep until they turn 25. (Office custody)
- Contracts/leases: keep seven years. (Office custody)
- Corrective action requests: keep two years. (Office custody)
- Financial records (audits, budgets, receipts, cheques, petty cash): keep seven years. (Office custody)
- Management review (minutes, agendas, monthly reports): keep two years. (Held on PCs by meeting type)

Your rights and how to make a complaint 📞

This section tells you about your rights and how to complain.

- You have the right to privacy and to see your records.
- You can ask us to correct information if it is wrong.
- We will support you to access your information.
- If you are unhappy, you can make a complaint.
- Tell DIRECTOR if you want to complain.
- We keep a Complaints Register and follow our Complaints Policy.
- You can have a family member, advocate or support person help you make a complaint.
- We will respond to complaints fairly and quickly.
- If the law requires, we may have to share information without your consent (for example child protection, reportable incidents or court orders). We will only share what is needed.

Responsibilities of The Company and staff 👥

This section tells you what we must do.

- The Company must keep systems that protect privacy and security.
- DIRECTOR keeps policies up to date and controls access to records.
- Staff must follow this policy and keep good records.
- Staff must protect participant privacy and confidentiality.
- Staff must report concerns or incidents to DIRECTOR.
- All staff are invited to suggest improvements to our processes.

If you want more information or help, please contact DIRECTOR.