

2.4 Information Management

Information Management Policy and Procedure

1.0 Purpose

121 Supports Hunter Pty Ltd actively works towards implementing and operating effective communication processes and information management systems. We strive to maintain all information systems and practices following legislative, regulatory compliance and organisational standards.

2.0 Scope

The policy of 121 Supports Hunter Pty Ltd is that all participants, staff, volunteers and contractors will have records established upon entry to the service while actively engaging with 121 Supports Hunter Pty Ltd.

3.0 Policy

- 121 Supports Hunter Pty Ltd will maintain effective information management systems that control stakeholders' appropriate privacy and confidentiality.
- 121 Supports Hunter Pty Ltd will abide by the Australian Privacy Principles (APP), including
 - 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

- 121 Supports Hunter Pty Ltd's policies and procedures are stored as read-only documents in the Policies and Procedures folder on the shared drive.
- 121 Supports Hunter Pty Ltd is responsible for maintaining the currency of this information with assistance from the General Manager and other staff members, as required.
- The involvement of all staff members is encouraged to ensure 121 Supports Hunter Pty Ltd's policies and procedures reflect best practices and foster ownership and familiarity with the material.
- A copy of each form our organisation uses is maintained in The Company Data SharePoint Folder under the relevant section
- All staff can access the policies and procedures at 121 Supports Hunter Pty Ltd's office in a paper-based or electronic format.
- At a minimum, policies and procedures are reviewed every three (3) years.
- All superseded policies and procedures are deleted from 121 Supports Hunter Pty Ltd's Policy and Procedure folder and electronically archived by the General Manager or a delegate.

4.0 Procedure

4.1 121 Supports Hunter Pty Ltd information management system

4.1.1 Participant documentation procedure

- Participants are informed of the following:
 - reasons for collecting personal information
 - use and disclosure of personal information
 - security of their information
 - the management of their information
 - government requirements, e.g. opt-out
 - access to their information
 - how to change any details
- Confidentiality of participant records is maintained.
- All 121 Supports Hunter Pty Ltd staff and volunteers responsible for providing, directing or coordinating participant support must document their activities.
- Participant files will provide accurate information regarding their services and support and will contain, but are not limited to:
 - participant personal details
 - referral information
 - assessments
 - support plans and goals
 - personal emergency preparation plan
 - participant reviews

- details regarding service responses.
- Original participant documentation is stored in the participant's central file.
- Information relating to a participant's ongoing situation, including changes to their situation (e.g. increased confusion, deteriorating health, increased risk), must be documented in their notes.
- All staff are appropriately trained in documentation and record-keeping (Etrainu Module)
- Staff must clearly understand the participant's requirements, goals, and strategies, including information within the support and emergency plans.
- Individuals are not permitted to document on behalf of another person.
- Participant records will be audited regularly to ensure thorough, appropriate, and high quality.
- Participant records will be stored in a safe and secure location with access available to authorised persons only.
- Service agreements must be maintained per the participant's NDIS plan and provided according to the participant's communication needs.
- Agreements with brokerage agencies will require brokerage workers to document their activities regularly.
- Staff must enter notes and observations into the participant's file in a factual, accurate, complete and timely manner.
- Staff members must only use information collected from a participant for the purpose it has been collected.
- Participants should be advised that the organisation may use data that has been collected but does not identify any participant for service promotion, planning or evaluation.
- Participants, families and advocates have a right to access their personal information collected, and staff will support such persons to access their personal information as requested.

4.1.2 Entering 121 Supports Hunter Pty Ltd's service

Upon a participant entering our service, all initial information will be collected using 121 Supports Hunter Pty Ltd's Participant Intake Referral Form. Only personal information will be collected to assess and manage the participant's support needs.

The 121 Supports Hunter Pty Ltd's Assessment Report will be used to document the participant's assessment information. A Participant Individual Risk Assessment will be undertaken to develop the Person Centered Plan and the Participant Emergency Plan.

In the case of Support Coordination only Participants the Support Coordination Plan (with included Risk Assessment) and Participant Emergency Plan will be developed

121 Supports Hunter Pty Ltd's Community Engagement Coordinator/ Community Services Manager (Participant Inclusion) will work with the participant, their advocate/s and any other family or service

providers/individuals to develop and document a participant support plan; this will be documented using 121 Supports Hunter Pty Ltd's Support Plan.

A participant file will be created as the central repository of all participants' service information and interactions. Each participant may be assigned a unique identifier for documentation and record-keeping purposes.

The participant's file will only contain material relevant to the management of services or support needs, including, but not limited to:

- copy of the signed agreement
- assessments
- risk assessment – individual and environment
- health reports
- the Person Centered Support Plan
- the Participant Intake Referral Form
- communication notes
- the Participant Information Consent Form
- the Participant Emergency Plan
- complaint information.

4.1.3 Ongoing documentation procedures

121 Supports Hunter Pty Ltd's ongoing documentation procedures include:

- maintaining participant information in Brevity CSM system, following system practices
- documenting participant information and service activities only on 121 Supports Hunter Pty Ltd's approved forms or tools
- updating of documents at review and during any emergency or disaster
- ensuring other service agencies and health professionals involved with the care or support of 121 Supports Hunter Pty Ltd's participant provide adequate documentation of their activities and the participant's wellbeing or condition.

The type of detailed information documented includes:

- outcomes of all ongoing participants assessments and reassessments
- changes or redevelopment of a participant's support plan, including revised goals or preferences
- critical incidents or significant changes in the participant's health or wellbeing
- emergency or disaster considerations (e.g. health order, natural disaster)
- conversations, in person or via telephone, with a participant, family members, their representative or advocate

- conversations regarding the participant, with any other providers, agencies, health/medical professionals, family members or other individuals with interest in the participant
- activities associated with the participant's admission and exit, including referrals.

4.1.4 Setting up and maintaining files for participants

Once a personal file for a participant is established, staff must maintain that file to ensure that all information is accurate, up-to-date and complete:

- relevant staff must document significant issues and events that arise during their work with the participants as the events and problems occur
- non-current (information that no longer has any bearing on the services provided to the participant), staff will establish an archival file and progressively cull non-current information into that file for secure storage.
- regular file audits by General Manager ensure that:
 - files are up-to-date
 - forms are being used appropriately
 - non-current information is being culled and stored in the archival file
 - progress/file notes are factual, accurate, complete and in chronological order
 - risk plan is current
 - a Participant Emergency Plan is relevant, trialled and used to inform management.
- exiting the service – all files - personal and archival will be stored in a secure place such as a locked area or password-protected folder on a computer under the control of 121 Supports Hunter Pty Ltd.

4.1.5 Participant file formats

- The files of participants will be established and maintained in the following format:
 - a standard manila folder, or another similar folder, or
 - held in a secure electronic format with password access.
- The forms must be based on the current formats approved by 121 Supports Hunter Pty Ltd.
- Archival files may be:
 - in lever-arch folders or archive boxes and multiples as required
 - electronically in the approved forms/domains and formats
- For ease of access, materials in the archival file should be listed chronologically, with each page numbered in order and groups of similar forms.

4.1.6 Security of files and participant information

- All current hard copy files for participants must be kept in a secure area, such as a lockable filing cabinet at the service, ensuring only authorised personnel can access a participant's personal information.

- Authorised personnel include 121 Supports Hunter Pty Ltd's employed staff members to support the participants. If files cannot be stored at the service, then alternative arrangements will need to be made by the participant and the Director to ensure confidentiality and security.
- All electronic files must be password protected to ensure confidentiality and security.
- If stored at the service, current participants' files can only be taken by relevant staff members from 121 Supports Hunter Pty Ltd to provide the participant's information or access to another service, such as a doctor.
- Non-current files should not be removed from the service unless:
 - they are being moved to a more secure archival storage unit
 - permission has been sought from the Director to do so.
- Staff must not undertake any of the following actions without the express approval of the Director:
 - photocopying any confidential document, form or record
 - copying any confidential or financial computer data to any other computer, USB or storage system such as Google Docs
 - communicate any confidential data to any unauthorised staff member or any other person/s.

4.1.7 Transporting a participant's hard copy files

When a participant's hard copy files need to be transported from one location to another (e.g. from their usual site to a doctor), they must be carried in a locked document container (e.g. a briefcase or attaché case). 121 Supports Hunter Pty Ltd will provide the staff with a locked case, as required.

4.1.8 Communication/file notes for participants

- Communication/file notes for participants must include the following components:
 - the date the entry is made
 - the time when the entry is being made
 - the time when the event occurred
 - nature of the event in a factual, accurate, complete and timely manner
 - signature of the person making the entry
 - the surname of the person making the entry (printed in brackets)
 - person's position of employment.
- Staff must ensure that all relevant information about the participant is entered into the person's file notes in a factual, accurate, complete and timely manner.
- The file notes for each participant should be written when a significant event occurs or to record the type of support provided while working with a participant. The definition of a significant event will vary from person to person and should be determined in consultation with the Director and should relate to the support required by the person-centred plan.

- It is required that staff make an entry in the file notes on each workday, even when the person's day has gone according to plan and without unusual or extraordinary events.
- All entries into file notes should be placed on the next line. Under no circumstances should blank spaces be left on the file notes sheet.
- On behalf of another staff member (e.g. dictating over the phone), all file note entries made by staff members must be signed by the person dictating the notes on their next shift. It is that person's responsibility to check the entry for accuracy and, if required, note any corrections that need to be made on the next line available.
- The participants should be aware of what has been recorded in their progress/file notes whenever required.

4.1.9 Working from home

Staff who work from home must sign the Privacy and Confidentiality Agreement. The security requirements for working from home include:

- only the staff member can access any documents, both written and electronic
- the computer must have a firewall to protect information
- all information linked to the server must be uploaded at the end of the day.
- start and finish times are to be recorded and sent to the supervisor
- report current work status at least weekly.

4.1.10 Access to participants' files

- Participants/guardians are provided access to their records on request. The Director should approve and control how participants access their files to maintain the security of other non-related information.
- Access to a participant's file is the direct responsibility of the Director. When access is requested by anyone other than 121 Supports Hunter Pty Ltd staff, Director will grant permission when the policies and procedures have been followed and access to the file is in the participant's best interest. Such access will only be granted when the appropriate person has given consent.
- All participants' files are the property of 121 Supports Hunter Pty Ltd and, although a participant and their guardian can access the file, it cannot be taken by a participant or guardian; or be transferred to any service external to 121 Supports Hunter Pty Ltd without permission of the Director.
- Copies of legitimately released files for any reason shall be recorded on an appropriate letter, which shall be signed as a receipt by the service recipient or their legal guardian. Our Consent Policy and Procedure outlines the proper procedure for releasing information about a participant to persons or services external to 121 Supports Hunter Pty Ltd.

- Any students on placement at 121 Supports Hunter Pty Ltd may only access files with the participant's consent or their guardian. Students must always provide a written undertaking to maintain confidentiality and only use non-identifying information. This agreement is to specify what information is to be used for and advise that any written compositions containing information are to be provided to the Director for approval before dissemination.

4.2 Staff records

Staff files are kept in a filing cabinet in the General Managers office and are available only to the Director. The filing cabinet is locked when the office is unattended.

- The staff files will be established and maintained in the following format:
 - a standard manila folder, or another similar folder, or
 - held in a secure electronic format with password access.

4.3 Minutes of meetings

Minutes of meetings are maintained on the shared drive in an identifiable folder, e.g. Management Meetings. The minutes must be identified:

- with meeting title, e.g. Management Meeting
- by date, e.g. Management Meeting/12/0X/YY
- saved as Management Meeting (date)

4.4 Other administrative information

Individual staff members are responsible for organising and maintaining the filing of general information following their position descriptions.

Administrative information, including funding information, financial information and general filing, is maintained in the filing cabinets in the General Managers office. The cabinets are locked when the office is unattended for a lengthy period, and all electronic files are password secured.

4.5 Electronic information management

4.5.1 Data storage

- All data is stored in the shared drive of the server.
- The General Manager is the only person who can add new data folders to the server's shared drive.

4.5.2 Backup

- All computer data (including emails) is backed to a remote server every night.
- Periodic testing of backed-up data is undertaken to check the system's reliability.

4.5.3 External programs

No programs, external data or utilities are installed onto any workstation without the permission of the General Manager.

4.5.4 Log-in credentials

Log-in credentials are assigned by the General Manager or their delegate.

4.5.5 Email

- Staff should not send and receive personal emails unless approved by Director
- All emails are filed in the appropriate folders
- Pornographic, sex-related or spam email received is to be deleted immediately. Under no circumstances are staff allowed to open or respond to spam emails.

4.5.6 Internet access

- Internet access is restricted to work-related purposes.
- Internet access reports are maintained on the server and are regularly reviewed by the Director.
- Under no circumstances are staff allowed to access pornographic or sex-related sites.

4.5.7 IT Support

- Our organisation maintains an ongoing IT support agreement with Dyn IT Pty Ltd.
- If staff experience problems with a program, computer, or any other piece of IT equipment, they can, in the first instance, contact the General Manager
- If necessary, the General Manager will arrange for the IT consultant/s to assist.

4.5.8 Social media

- Our organisation is aware that social media, e.g. social networking sites such as Facebook, Twitter or similar, video and photo-sharing sites, blogs, forums, discussion boards and websites, promote communication and information sharing.

- Staff are required to ensure the privacy and confidentiality of the organisation, participants and their information.
- Staff must not access inappropriate information or share any information on their work through social media sites.
- All staff are required to seek clarification from the Director if in doubt as to the appropriateness of sharing any information related to their work on social media sites.

4.6 Monitoring information management processes and systems

We regularly audit information management processes and systems as part of our audit program. Staff, participants and other stakeholders are encouraged to provide ongoing feedback on issues and areas where improvements are possible.

4.7 Archival and storage

After their active period, all records must be kept in the archive files for an additional time. Regulatory, statutory, and legislative requirements determine the retention period, or as defined by 121 Supports Hunter Pty Ltd as a best practice (refer to Attachment 1: Disposal and archiving of documents).

Archived records must be identified and stored to allow easy access and retrieval when required. Archived records, in hard copy, must be stored in an environment that minimises deterioration and damage, i.e. not exposed to direct sunlight, moisture, extremes of temperature, pests, dust and fire hazards.

4.8 Destruction of records

The following procedures apply for the destruction of records:

- As required, junk mail and instructional post-it notes may be placed in recycling or other bins.
- All other records or documents requiring destruction are to be:
 - Put in the Mobile Shredding company Bin at 121 Supports Hunter Pty Ltd Office.
 - This will be picked up to be securely pulped
 - deleted from the network.

5.0 Related documents

- All electronic and hard copy documentation
- 121 Complaints Register
- 121 Service Agreement
- Privacy Statement - Website
- 121 Participant Intake Referral Form

- 121 Participant Information Consent Form
- 121 Participant Emergency Plan
- 121 Person Centered Support Plan
- Consent Policy and Procedure

6.0 References

- Disability Discrimination Action 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

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
Participant records	Name Address Telephone number Emergency Contact Application Complaints about the 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
Management review	Minutes of meetings Agendas Monthly reports	Two years	Held on PCs according to the type of meeting