Policy B-01

Supporting Client Information

Just Support Services ensures that all client information is accurate, current, secure and accessible to authorized persons and is managed in a way that supports safe, high-quality service delivery while protecting the rights and privacy of the individual.

1. Purpose

a) This policy outlines the procedures on how participant information is managed in the collection, collation, reporting, security and access to client files.
b) It is relevant to hard copy and electronic files.

2. Responsibilities

a) All staff and workers are responsible for ensuring that the contents of files are up to date, accessible, accurate, stored securely and maintained to company policy.
b) Management are responsible for conducting annual file audit to monitor client information and its relevance.

3. Definitions

a) **Vertex360:** The company's Client Record Management database used for client information, service details, scheduling/rostering of supports, reporting of incidents and storage of files.
b) **CRM:** Client Record Management System
c) **Hard Copy Files:** Information stored on paper including documents and images.
d) **Electronic Files:** Information recorded in a manner that requires a computer or other electronic device to display, interpret and process it.
e) **Eligible Data Breach:** Unauthorized access to or unauthorized access of personal information, or loss of personal information, that an agency holds, that is likely to result in serious harm to one or more individuals
f) **Operations Manager:** The person responsible for managing and controlling all day-to-day operations of the company and hold the most senior management position.
g) **Staff:** Person directly employed by the company.
h) **Worker:** Person brokered via contract to provide services to the company under signed agreement.
i) **Participant:** Person in direct receipt of services and supports from the company.
j) **Client:** Any person engaged with the company in direct or indirect receipt of service. For example, participant, an informal partner organization or carer of person receiving supports.

4. Policy Statement and Procedures

General:

a) Files are maintained for all persons in receipt of services and support from Just Support Services. The information held is dependent on the service provided. As a minimum, the company will collect and maintain:
   - Personal Information (name, date of birth, gender, address, contact details, disability, health conditions, next of kin, country of birth, cultural identity, preferred language/communication, living/accommodation arrangement)
   - Goals/Service Plan
   - Service Notes/Communication
   - Risk Profile (when determined as relevant)
   - Support Plans/Protocols (when determined as relevant)

b) There are procedures in place for the review, storage and archiving of client information as per B-07 Client Information Audit.

c) Information relevant to the service type, level of support, legal and funding body requirements is collected and stored in participants or client files.

d) All staff, workers and management are responsible for information being stored to be accurate and up to date. Reports must be written in an objective and unbiased manner. No information is to be removed from a client/participant file except in line with archiving and file destruction procedures, and no records can be falsified.

e) Files are audited regularly by Managers to ensure information is correct and stored in line with policy.

f) Staff are responsible for entering records in a timely manner in a way that remains objective, factual and non-judgmental

g) Management are responsible for ensuring system access controls are maintained and documentation meets compliance standards

Hard Copy Files:

Hard copy files are a secondary source of information only.

a) Hard copy files are created only when it is not possible to use existing electronic file processes due to access, or to meet the preferred communication need of the client/ participant.

b) In this case, the required documentation will be produced in hard copy and provided to the client/ participant for implementation with workers. This will generally be limited to service plans and supporting protocols.

c) Hard copy files may be used for temporary store of manually completed documents where there is no option for electronic completion. These documents are transferred to the electronic system as soon as practicable after completion.

d) All information is clear and legible and includes client name, date and name, position and signature of person completing.

e) When reviewed without change, this is clearly recorded with the date of review, name, position and signature of reviewer.

f) Hard copy documents in participant homes will be updated with the yearly review, or on request due to a change in circumstance or supports.

g) Hard copy documents must be scanned and uploaded to the electronic system as soon as possible.

File Audit:

a) Files will be audited annually in line with Form B-08 Client Information Audit for all participants receiving regular ongoing support.
b) An independent audit will be completed by a secondary staff member not responsible for the file, to verify that files are being maintained. The number equivalent to 20% of total files will be audited as sample.
c) Any improvements identified by the secondary staff memeber will be corrected by the Service Manager and repeated should more than 50% of the sample not meet file audit requirements.

Security of Client Information:

a) Client files are stored as per A-07 Privacy and Confidentiality policy.
b) Hard copy files are stored in locked cabinets away from general access.
c) Electronic files are secured through role-based access controls, password protection and system level security measures. This includes individual worker, staff or manager log in codes, access restrictions based on position, ability to lock documents, files and folders and virus protection.
d) If a hard copy file is taken off site, staff must ensure client information is not visible to unauthorized persons when transported or accessed offsite.
e) All suspected or actual data breaches must be reported immediately to management. Breaches will be assessed, contained and managed in accordance with the Notifiable Data Breach Scheme, including notification to the OAIC and affected individuals where required. Fact Sheet Notifiable Data Breach
f) Just Support Services maintains custody of records; however participants have the right to access their personal information in accordance with privacy legislation.
g) Assessments or Support Plans/Protocols completed with the participant, or provided by the participant remain their property and require consent to share with others external of Just Support Services.

Access to Client Information:

a) All requests for access to a client or participants' file must be referred to the Operations Manager. The request will be discussed with the participants, client or their authorized representative and consent obtained to release information.
b) Except in the case of a subpoena all requests must be consented by the client or their representative.
c) Requests for access will be responded to within a reasonable time frame.
d) Access may be limited where it would pose a risk or breach the privacy of others, in accordance with legislation.
e) A record of information sent must be made in the client's Vertex360 file including who requested/received the information, what was sent and the date. Original documents should not be provided to third parties.
f) Participants and the guardians are able to access their files and copy information within the file. This access will be under the supervision of management.
g) Client information may be transmitted electronically where appropriate security measures are in place (e.g. secure email, password protection, encryption)

Subpoena for Client Information:

a) The subpoena does not require client consent to be obtained, and will specify the required information.
b) Only the Operations Manager may respond to the request and will make a determination as to the requirement for legal advice.

Archiving and File Destruction:

a) Documents in client files are archived when a more recent version is available, or at least annually for non-current information including client notes, recorded data and rosters of support.
b) Archived documents are to be recorded in the file (hard and electronic) and if hard copy the files is maintained in a locked cabinet in secure premises.
c) Archived information is to be destroyed or permanently deleted in line with the following schedule:
    - Adult participants – seven years after permanent exit from service
    - Child participants – seven years after the child turns 18 or seven years after permanent exit from the service (the longer period applies)
    - Information relating to the assault of abuse of a child is maintained indefinitely
d) Destruction of files must be in accordance with legislative and regulatory requirements including ensuring secure destruction (e.g. shredding, permanent deletion)

5. Forms and Records

Form A-03 Approval to Disclose Information

Form B-08 Client Information Audit

6. Work Instruction and Safe Working Procedures

Nil

7. Related Policies

A-07 Privacy and Confidentiality

B-07 Client Information Audit

8. Related Documents

Fact Sheet – Notifiable Data Breach

9. References

Privacy Act (Commonwealth) 1988

State Records Act (NSW) 1998

Privacy Amendment (Notifiable Data Breaches) Act 2017

Australian Standards ISO 15489 Records Management