P032 – PARTICIPANT RECORDS POLICY

1. Scope

This policy applies to Management, managers, staff, contractors and volunteers who manage and/or have access to participant files.

2. Policy Statement

District 360 ensures that all information necessary for the management of participant needs and the smooth operation of the service is maintained on participant files.

3. Purpose

This procedure defines how we manage participant files including the information collected, security & access and archiving and file destruction. The policy includes both hard copy and electronic files.

4. Responsibilities

Staff are responsible for maintaining files and ensuring that the contents are accessible, accurate and up to date and that they are stored securely.

Management is responsible for conducting annual file audits to monitor participant files.

5. Definition

Electronic files: any information stored in a form accessible through a computer or other electronic device. This includes word processing documents, spreadsheets, database files, charts, graphs, e-mail, text messages and PDF files. They can be stored on a computer, computer server, disks, USB & other portable drives, mobile phones, PDA's or other devices.

Hard Copy Files: information stored on paper including documents and photos.

6. Requirements

General

Participant Files are maintained for all participants receiving service from District 360 excluding Information Services and Sports Ready. The amount of information held is dependent on the service provided but the following basic information will be maintained:

- Personal Information (name, age, address, disability, contact details, next of kin).
- Risk Profile (assessments, reports and plans).
- Support Plans (service contracts, individual plans, care plans,).
- Health/Medical & Behaviour Support (where applicable).
- Service Details (activities, rosters, programs, employment).
- Participant Notes, Communication & Correspondence.

- Finance or Wages.

District 360 procedures of management of participant files including defining what information is collected and how it is accessed, stored, retrieved, reviewed and archived.

Only information relevant to the provision of services to the participant and our legal responsibilities to the participant and others will be held on participant files. Information not relevant to service provision will be either returned to the participant or destroyed dependant on the nature of the information.

Staff are required to ensure that participant documents are accurate and up to date. All reports must be written in an objective and unbiased manner.

No information is to be removed from a participant file except in line with archiving and file destruction protocols.

Falsifying participant records will result in disciplinary procedures. (Refer to P022 Disciplinary Procedures Policy).

Files are to be audited regularly by Managers to ensure information is up to date and easily accessible. (Refer to F016 Participant File Audit Checklist).

All staff are to receive information at induction on the appropriate maintenance of participant files. Additional training is to be provided periodically.

Information is to be scanned and saved into the secure network drive and hard copies to be filed in the individual participant folder.

Electronic and hard copy files are to be set up with an individual participant folder and appropriate sub folders;

PARTICIPANT FOLDER	SUBFOLDERS	FORMS/DOCUMENTS
Joe Blog	INITIAL	☐ Referral Form
		☐ Participant Assessment form
		☐ Participant Profile
		☐ Privacy statement
		☐ NDIS consent form
		☐ Image consent form
	AGREEMENT	☐ Service Agreement
	FUNDING	☐ Funding Document (NDIS Plan/s)
	SUPPORT PLAN	☐ Individual Plan
		☐ Support Coordinator Report
	FEEDBACK	Incidents reports, service feedback, case notes, progress notes, assessments
	COMMUNICATION	Emails, letters, phone call records, etc.
	ACCOUNTS	Invoices to claim
	EXIT	Exit form

All information is to be documented in clearly legible formats.

All internal documents placed in participant files must include the participant's name, the date and the name, position and signature of the author. All other documents must be dated and include the participant's name.

Where a section of a file or document is not relevant it should be clearly marked as 'Not Applicable'. Unused lines or spare space should be crossed through.

Where a document is reviewed without change, it should be clearly recorded that this has occurred including the name, date and signature of the reviewer.

Handwritten reports and documents are not to be rewritten or typed (excluding draft documents). File Auditing

An annual audit is to be conducted of all files for participants receiving regular ongoing support.

In addition to the annual file audits an independent audit is conducted to verify that the files are up to date. The square root of the total number of files will be audited as a sample.

All systems improvements identified by the independent audit will be corrected by the Service Manager and the audit repeated should the sample not comply with District 360 policies and procedures. Security & Access

Participant files and sensitive information is stored in accordance with the Privacy and Confidentiality Policy. (Refer to P003 Privacy & Confidentiality Policy).

Hard Copy files are stored in locked cabinets or drawers away from general access areas.

Electronic files are secured in line with the Information Technology Policy to prevent inappropriate access. These measures include individual employee log-on codes, access restrictions based on position and section, facilities to lock documents and folders, virus protection, fire walls and server log-on protection.

When transporting participant files, appropriate measures must be taken to ensure their security.

When participant files are taken off-site a record of this must be kept in the in the participant's electronic file and, if appropriate, in the file's normal location.

In the event that participant information is lost or stolen, participants and/or families are notified in writing as soon as possible.

- They should be informed about the type of information that was stolen and what the service has attempted to do to retrieve it.
- An incident report is to be completed for any instance involving loss of participant files or information.

All reports, programs and other documentation completed during the course of service provision remain the property of District 360.

Participants may access their files and can copy any information contained within these files. Participants are asked to make a time to come into the office so as to ensure that someone is available who can access the file for them.

Where a participant is unable to give informed consent regarding file access, a guardian or person responsible may access the files and can copy any information contained within these files. They are asked to make a time to come into the office so as to ensure that someone is available who can access the file for them.

Participant files and sensitive information is shared only in accordance with the Privacy and Confidentiality Policy. (Refer to P003 Privacy & Confidentiality Policy). This includes the provision of information in verbal, written or electronic format.

Information from participant files and other highly confidential information should not be transmitted via Email or Internet without appropriate security measures. Where required for the purposes of job search for participants, resumes containing some personal details may be submitted to potential employers with the permission of the participant concerned. District 360 will transmit such information only with the consent of the participant. District 360 cannot assure the integrity of information transmitted electronically.

Archiving and File Destruction

Information from participant files should be archived in line with the following schedule:

- Immediately on a document being superseded by a more recent version.
- Annually or more often if required all non-current information should be archived. This includes participant notes, medication sheets, routine correspondence, financial records, medical reports, rosters and activity plans.
- A record of archiving activities is to be maintained in the participant's file.
- Files are to be archived into clearly marked folders. Where a participant receives infrequent service, archives may be held in their primary file in a section clearly marked as archives and with appropriate tabs.
- Archived files are maintained in locked cabinets in secure premises.
- Information from archived files should be destroyed in a manner commensurate with privacy protection in line with the following schedule:
    - Adult consumers - 7 years after exit from a service.
    - Children's files - 7 years after the child attains the age of 18 years or 7 years after they exit the service, whichever is the longer.

- Files relating to the abuse or assault of a child are maintained indefinitely.

7. Other relevant District 360 policies and forms

Staff, especially managers and supervisors, are encouraged to read this policy in conjunction with other relevant District 360 policies, including;

- Privacy and Confidentiality Policy
- Disciplinary Procedures Policy

Relevant Forms;

- Participant File Audit
- Incident Report

8. Related legislations and Standards;

- Privacy Act (Commonwealth) 1988
- State Records Act (WA) 2000
- Freedom of Information Act 1992 (WA)
- The Information Privacy Bill 2007 (WA)
- The Privacy Act 1988
- Australian Standards ISO 15489 Records Management
- Evidence Act (Commonwealth) 1995

9. More information

If you have a query about this policy or need more information, please contact the management team at info@district360.com.au

10. Review details

Approval Authority	Tanya Johnston
Responsible Officer	Coco Johnston
Approval Date	14 April 2021
Last updated Date	30 July 2024
Next Review Date*	30 July 2025
Last amended	- Reviewed the up to datedness of the information.