THE DISABILITY TRUST

Policy D-07
Managing Client Files

1.0 Policy

The Disability Trust ensures that all information necessary for the management of client needs and the smooth operation of the service is maintained on client files.

2.0 Purpose

2.1 This procedure defines how we manage client files including the information collected, security & access and archiving and file destruction.

2.2 The policy includes both hard copy and electronic files.

3.0 Responsibilities

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

3.2 Management are responsible for conducting annual file audits to monitor client files.

4.0 Definitions

4.1 *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.

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

5.0 Requirements

General

5.1 Client Files are maintained for all clients receiving service from The Disability Trust excluding Information Services and Sports Ready. The amount of information held is dependant 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).
- Client Notes, Communication & Correspondence.
- Finance or Wages.

5.2 Each division of The Trust has procedures for the management of client files including defining what information is collected and how it is accessed, stored, retrieved, reviewed and archived.

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

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

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

5.6 Falsifying client records will result in disciplinary procedures. (See Policy F-12 Managing the Disciplinary Process).

5.7 Files are to be audited regularly by Managers to ensure information is up to date and easily accessible. (See Form-D-07-01 Client File Audit).

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

5.9 Information is to be placed directly into Hard Copy Files. Plastic sleeves are not to be used and loose documents are not to be left in files. Information that cannot be hole-punched should be placed in a zippered document pouch.

5.10 Electronic files are only to be used as a primary storage mode where the system contains an automatic date and signature function (e.g. Carelink). Files without this function do not form a legal record.

5.11 Other electronic files are to be set up with an individual client folder and appropriate sub folders.

Documentation

5.12 All information is to be documented in clearly legible formats.

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

5.14 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.

5.15 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.

5.16 Hand written reports and documents are not to be rewritten or typed (excluding draft documents).

File Auditing

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

5.18 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.

5.19 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 The Disability Trust policies and procedures.

Security & Access

5.20 Client files and sensitive information is stored in accordance with the Privacy and Confidentiality Policy. (See Policy C-02 Privacy, Dignity & Confidentiality).

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

5.22 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. (See Policy K-02 Information Technology).

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

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

5.25 In the event that client information is lost or stolen, clients 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 client files or information (see Form H-10-01 or 'Riskman')

5.26 All reports, programs and other documentation completed during the course of service provision remain the property of The Disability Trust.

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

5.28 Where a client 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 in to the office so as to ensure that someone is available who can access the file for them.

5.29 Client files and sensitive information is shared only in accordance with the Privacy and Confidentiality Policy. (See Policy C-02 Privacy, Dignity & Confidentiality). This includes the provision of information in verbal, written or electronic format.

5.30 Information from client 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 clients, emailed resumes containing some personal details may be submitted to potential employers with the permission of the client concerned. The Disability Trust will transmit such information only with the consent of the client. The Trust can not assure the integrity of information transmitted electronically.

Archiving and File Destruction

5.31 Information from client 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 client notes, medication sheets, routine correspondence, financial records, medical reports, rosters and activity plans.

5.32 A record of archiving activities is to be maintained in the client's file.

5.33 Files are to be archived into clearly marked folders. Where a client receives infrequent service, archives may be held in their primary file in a section clearly marked as archives and with appropriate tabs.

5.34 Archived files are maintained in locked cabinets in secure premises.

5.35 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.

6.0 Forms and Records

Form-D-07-01 Client File Audit

Form-D-10-01 Incident Report

7.0 Work Instructions and Safe Working Procedures

WI-D-07-02 Client Files - Respite & Community Services

8.0 Related Policies

C-02 Privacy, Dignity & Confidentiality

K-02 Information Technology

9.0 Related Documents

Nil

10.0 References

Privacy Act (Commonwealth) 1988
State Records Act (NSW) 1998
Privacy and Personal Information Protection Act (NSW) 1998
Information Privacy Act 2014 (ACT)
Health Records Information Privacy Act (NSW) 2002
Australian Standards ISO 15489 Records Management
Evidence Act (Commonwealth) 1995