9.3 Information Management Policy and Procedure

Procedures number:	9.3	Version:	1.0
Drafted by:	ML, BV, TV	Endorsed by Board on:	June 2020
Responsible person:	EO	Scheduled review date:	June 2021

PURPOSE

Interchange IE actively works towards implementing and operating effective communication processes and information management systems. We strive to maintain all information systems and practices in accordance with legislative, regulatory compliance and organisational standards.

SCOPE

It is the policy of Interchange IE that all participants, staff and volunteers will have records established upon entry to the service and maintained while active at Interchange IE.

POLICY

Interchange IE will maintain effective information management systems that keep appropriate controls of privacy and confidentiality for stakeholders.

- Interchange IE's policies and procedures are stored as read-only documents in the Policies and Procedures folder on the shared drive with relevant policies being available on the Interchange IE website.
- Interchange IE is responsible for maintaining the currency of this information with assistance from the Executive Officer and other staff as required.
- The involvement of all staff is encouraged to ensure Interchange IE's policies and procedures reflect best practice and to foster ownership and familiarity with the material.
- All staff can access the policies and procedures at Interchange IE's office in a paper-based (on request) or electronic format.
- Policies and procedures are reviewed every three (3) years at a minimum, or as required.
- All superseded policies and procedures are deleted from Interchange IE's Policy and Procedure folder and electronically archived by the Executive Officer or a delegate.
- Interchange IE Board of management can access up to date Interchange IE policies and procedures electronically

PROCEDURE

Interchange IE information management system participant documentation procedure;

- Confidentiality of participant records is to be maintained.
- All Interchange IE's staff and volunteers responsible for providing, directing or coordinating participant support must document their activities.

Participant's files will provide accurate information regarding their services and support and will contain, but is not limited to:

  - participant's personal details
  - assessments
  - support plans and goals

- Participant documentation is stored in the participant's electronic file.
- All Interchange IE staff who are required to document the activities relating to support of participants will be appropriately trained in documentation and record-keeping.
- Individuals are not permitted to document on behalf of another person.

9.3 Information Management Policy and Procedure

- Participant records will be audited regularly to ensure documentation is thorough, appropriate and of high quality.
- Participant records will be stored in a safe and secure location with access available to authorised persons only.
- Staff must ensure that all relevant information about the progress of, or support provided to a participant, is entered into that participant's file notes in a factual, accurate, complete and timely manner.
- Staff must only use information collected from a participant for the purpose for which it has been collected.
- Participants should be advised that data which has been collected, but which does not identify any participant, may be used by the organisation for the purpose of service promotion, planning or evaluation.
- Participants, family and advocates have a right to access any of their personal information that has been collected. Staff will support such persons to access their personal information as requested. Interchange IE complies with its 'request to access personal information protocols', see below.

Accessing Interchange IE's service

Upon a participant accessing our service all initial contact - information will be collected using Interchange IE's Participant Intake form. Only personal information necessary to assess and manage the participant's support needs will be collected.

Interchange IE 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 Interchange IE's authorised template.

A participant file will be created to act as the central repository of all participant's service information and interactions. The participant's file will only contain material relevant to the management of services or support needs, including, but not limited to:

- a copy of their signed service agreement
- all relevant assessments
- participant intake form
- communication notes
- complaint information

Ongoing documentation procedures

Our ongoing documentation procedures include:

- maintaining participant information in electronic form, in accordance with organisational frameworks
- documenting participant information and service activities only on Interchange IE's authorised forms or templates
- ensuring other service agencies and health professionals, involved with the care or support of an Interchange IE's participant, provide adequate documentation of their activities and the participant's wellbeing, condition or circumstance upon request before proceeding with Interchange IE services.

The type of detailed information documented includes:

- outcomes of all ongoing participant 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
- activities associated with the participant's intake and exit, including referrals

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:

- As information in the personal file becomes non-current (information that no longer has any bearing on the services provided to the participant) staff will establish an archival file and regularly transfer non-current information into the archival file.
- Regular audit of participant files to ensure that:

9.3 Information Management Policy and Procedure

  - files are up to date
  - forms are being used appropriately
  - non-current information is being appropriately transferred and stored in the archival file
  - progress/file notes are factual, accurate, complete and in chronological order

When a participant leaves the service, their personal file will be electronically archived as per the requirements of the Interchange IE Document Control schedule.

Participant file formats

The files of participants will be established and maintained in the following format:

- The file will be stored in a secure electronic format
- The forms must be based on the current formats authorised by Interchange IE.
- Archival files will be electronic
- Any hard copies of documents will be transferred to electronic format then securely destroyed

Security of files and participant information

- Authorised personnel include Interchange IE's staff members who are employed to provide support to the participants. If files can't be stored at the service, then alternative arrangements will need to be made by the participant and the Executive Officer or their delegate to ensure confidentiality and security.
- Staff must not undertake any of the following actions unless in authorised circumstances that do not breach the participants right to privacy, and only when consent has been received:
  - 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
  - conveying any confidential data to any unauthorised staff member or to any other person/s.

Access to participants files

- Participants/guardians are provided access to their records on request. The Executive Officer or their delegate should approve and control the way participants access their files to ensure the security of other non-related information is maintained.
- Access to a participant's file is the direct responsibility of the Senior Manager. When access is requested by anyone, other than staff employed by Interchange IE it will only be granted when the Senior Manager is satisfied the policies and procedures of Interchange IE have been followed and access to the file is in the best interest of the participant. Such access will only be granted when the appropriate person has given consent.
- All participants files are the property of Interchange IE 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 Interchange IE without permission of the Executive Officer or their delegate.
- Copies of files that are legitimately released 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. The proper procedure for releasing information about a participant to persons or services that are external to Interchange IE is outlined in our 'Consent Policy and Procedure'.
- Any students on placement at Interchange IE may only access files with the consent of the participant or their guardian. Students will be required to provide a written undertaking that they will always 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 Executive Officer or their delegate for approval, before dissemination.

Staff records

Staff files are kept electronically on a drive that has limited access available only to HR and Senior Managers.

Minutes of meetings

Minutes of meetings are maintained in an electronic format on the shared drive.

9.3 Information Management Policy and Procedure

Other administrative information

Individual staff are responsible for organising and maintaining general information in accordance with their job descriptions.

Electronic information management

Data storage

All data is stored in the shared drive of the server.

Backup

- All computer data (including emails) is backed up every night to a remote server.
- Periodic testing of backed-up data is undertaken to check the reliability of the system.
- Deleted or lost items in the Cloud are retained for 93 days after being deleted.

External programs

No programs, external data or utilities are installed onto any workstation without permission.

Log-in credentials

Log-in credentials are assigned by the organisations IT provider

Email

- Staff are discouraged from sending and receiving personal emails.
- All emails are filed in the appropriate folders
- Pornographic, discriminatory, sex-related or spam email received is to be deleted immediately. Under no circumstances are staff allowed to open or respond to spam emails.

Internet access

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

IT Support

- Our organisation maintains an ongoing IT support agreement.
- If staff experience problems with a program, computer, or any other piece of IT equipment, support is available from our IT Support Provider or internally.

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 and volunteers who work in our organisation are required to ensure the privacy and confidentiality of the organisation's information and the privacy and confidentiality of participants and their information. Staff and volunteers must not access inappropriate information or share any information related to their work through social media sites.
- Staff and volunteers are required to seek clarification from their Manager, if in doubt as to the appropriateness of sharing any information related to their work on social media sites.
- Staff and volunteers are not to interact or communicate with participants on any form of social media except in authorised circumstances such as; online rostering, online support provision.

9.3 Information Management Policy and Procedure

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

Archival and storage
All records, after their active period, must be kept in archive files for an additional time. Regulatory, statutory and legislative requirements determine the retention period, or alternatively defined by Interchange IE as best practice (refer to 'Attachment 1: Disposal and archiving of documents').

Archived records must be identified and stored in a way that allows for easy access and retrieval when required.

Destruction of records
The following procedures apply for the destruction of records:

- Junk mail and instructional post-it notes may be placed in recycling bins or other bins as required.
- All other Interchange IE records or documents requiring destruction are to be:
    - shredded and or placed in secure disposal bin for destruction
    - deleted from the network.

Information Management Policy and Procedure

RELEVANT LEGISLATION AND POLICIES

Disability Discrimination Action 1992 (Commonwealth)

NDIS Practice Standards and Quality Indicators 2018

Privacy Act (1988)

Work Health and Safety Act 2011

RELATED DOCUMENTS

All electronic and hard copy Interchange IE documentation

Complaints Register

Consent Policy and Procedure

Copy of signed Service Agreement

Participant Intake Form

Participant Support Plan

Information Management Policy and Procedure

Attachment 1: Disposal and archiving of documents

Function/Activity	**Description**	**Retention/Disposal Action**	**Custody**
Aboriginal & Torres Strait Islander	Documents relating to Indigenous health. Normal operational documents.	Lifetime 7-years after the person's last contact with the service.	Office
Business information	Name Address Telephone number Compliance notices Financial records	7-years	Office
Internal audits	Audit schedule Audit questions Audit reports	2-years	Office
Participant records	Name Address Telephone number Emergency contact details Application or other documents Complaints about the non-delivery of services Incident records Complaint records BSP records	Lifetime - ongoing	Office
Contracts/leases	Properties, etc.	7-years	Office
Corrective action	Corrective action requests.	2-years	Office
Financial	Audits Budgets Receipts Cheques Petty Cash Documents and other financial records	7-years	Office
Management review	Minutes of meetings Monthly reports.	2-years	Held on PCs according to the type of meeting.