Information Management Policy and Procedure

PURPOSE

AACA 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

AACA's policy is that all participants, staff and volunteers will have records established upon entry to the service and maintained while active at AACA.

POLICY

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

- AACA'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 AACA website.
- AACA is responsible for maintaining the currency of this information with assistance from the other staff as required.
- The involvement of all staff is encouraged to ensure AACA's policies and procedures reflect best practices and to foster ownership and familiarity with the material.
- All staff can access the policies and procedures at AACA'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- All superseded policies and procedures are deleted from AACA's Policy and Procedure folder and electronically archived by the director or a delegate.
- AACA management can access up-to-date AACA policies and procedures electronically.

PROCEDURE

AACA information management system participant documentation procedure;

- Confidentiality of participant records is to be maintained.
- All AACA 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 are not limited to:
  - participant's personal details
  - assessments
  - support plans and goals
- Participant documentation is stored in the participant's electronic file.
- All AACA staff who are required to document the activities relating to the support of participants will be appropriately trained in documentation and record-keeping.
- Individuals are not permitted to document on behalf of another person.

- 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 that 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.

Accessing AACA's service

Upon a participant accessing our service all initial contact - information will be collected using AACA's Participant Intake form. Only necessary personal information for assessing and managing the participant's support needs will be collected.

AACA 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 AACA's authorised template.

A participant file will be created to act as the central repository of all participants' 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 AACA's authorised forms or templates
- ensuring other service agencies and health professionals, involved with the care or support of an AACA participant provide adequate documentation of their activities and the participant's well-being, condition or circumstance upon request before proceeding with AACA 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:
  - 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 AACA 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 AACA.
- Archival files will be electronic and hardcopy, depending on their importance and purpose.
- Any hard copies of documents will be transferred to electronic format and then securely destroyed.

Security of files and participant information

- Authorised personnel include AACA'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 director 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 participant's 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 director or their delegate 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 staff employed by AACA, it will only be granted when the director is satisfied that the policies and procedures of AACA 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 AACA 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 external AACA service without permission of the director.
- 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. Our ' Consent Policy and Procedure ' outlines the proper procedure for releasing information about a participant to persons or services that are external to AACA.
- Any students on placement at AACA may only access files with the participant's or guardian's consent. 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 director or their delegate for approval before dissemination.

Staff records

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

Minutes of meetings

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

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 to an external drive weekly.
- 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.

Email

- Staff are discouraged from sending and receiving personal emails.
- All emails are filed in the appropriate folders.
- Pornographic, discriminatory, sex-related or spam emails received must 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 director or their delegate.
- Under no circumstances are staff allowed to access pornographic or sex-related sites.

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 about 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 or support provision.

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

After their active period, all records must be kept in archive files for an additional time. Regulatory, statutory and legislative requirements determine the retention period or alternatively defined by AACA as best practice.

Archived records must be identified and stored to allow 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 AACA records or documents requiring destruction are to be:
    - shredded and or placed in a secure disposal bin for destruction
    - deleted from the network.

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 AACA documentation
- Feedback and Complaints Register
- Consent Policy and Procedure
- Copy of signed Service Agreement
- Participant Intake Form
- Participant Support Plan