

**Privacy, Dignity and Information Management Policy and Procedure**

**Policy**

Child and Adolescent Psychology Services will comply with:

* the Privacy Act 1988 and the Privacy Amendment Act 2012 to protect the privacy of individuals' personal information
* The [Office of the Victorian Information Commissioner](https://www.ovic.vic.gov.au/) (OVIC) which administers the [Privacy and Data Protection Act 2014 (Vic)](http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/vic/consol_act/padpa2014271/) and The [Office of the Health Services Commissioner](http://www.health.vic.gov.au/hsc/index.htm) which administers the [Health Records Act 2001 (Vic)](http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/vic/consol_act/hra2001144/) and conciliates complaints between consumers and health care providers.

This includes having in place systems governing the appropriate collection, use, storage and disclosure of personal information, access to and correction and disposal of that information.

The organisation is committed to protecting the privacy and dignity of its participants and staff.

Documents regarding participants will be written with consistency and accuracy. These documents will only be able to be accessed by authorised staff.

CAPS will ensure that participants are aware of the personal information that has been collected and that the participant consents to the collection of the information.

CAPS will ensure that:

* All legal and ethical obligations are met in protecting the privacy of participants and staff
* Participants are provided with information regarding their rights regarding privacy and confidentiality
* Participants and staff are aware of their rights when having personal discussions or meetings
* All staff are aware of the requirements in meeting their obligations surrounding participant privacy and dignity

**Outcome**

Compliance with legislative requirements governing privacy of personal information.

All Child and Adolescent Psychology Services participants are satisfied that their personal information is kept private and only used for the intended purpose

**Background**

The [*Privacy Act 1988*](http://www.comlaw.gov.au/Series/C2004A03712) (Privacy Act) is an Australian law which regulates the handling of personal information about individuals by private sector organisations. Amendments were made to this legislation in 2012 (the Privacy Amendment Act 2012) which updates the [Australian Privacy Principle](https://www.communityservices.act.gov.au/hcs/policies/information_privacy_principles_-_privacy_act_1988)s (APP) and came into effect in March 2014. The amendment requires an organisation to explicitly state how they will adhere to the APP and inform their participants on how their privacy will be protected. The APP cover the collection, use, storage and disclosure of personal information, and access to and correction of that information. The APP are summarised in Appendix 1 of this document.

**Definitions**

'Personal information' means information (or an opinion) we hold (whether written or not) from which a person’s identity is either clear or can be reasonably determined.

‘Sensitive information’ is a particular type of personal information - such as health, race, sexual orientation or religious information.

**Procedure**

*Ensuring all Child and Adolescent Psychology Services’ Staff Understand Privacy and Confidentiality Requirements*

1. The Director of Child and Adolescent Psychology Services will review their Privacy Policy annually and ensure they understand their responsibility to protect the privacy of individuals' personal information.
2. All Staff will undergo training related to Privacy and Confidentiality Requirements at the time of induction and then annually.

*Collecting Participant information*

1. Only collect information that is necessary for the functioning of the organisation and its supports
2. Use fair and lawful ways to collect personal information
3. Collect personal information only with the individual’s consent
4. Ensure that the individual knows what information is being collected, why it is being collected and who will have access to the information
5. Ensure that the information collected is accurate and up to date

*Privacy during interviews and personal discussions*

1. Only collect information that is necessary
2. Ensure the information is given voluntarily and stored securely
3. When possessing a document containing personal information’s, measures will be taken to ensure the document is not lost, accessed by unauthorised personal or modified or disclosed without authorisation
4. Discussions and meetings will be carried out with reasonable steps to ensure that the conversation is not over heard by unauthorised personel

*Managing Privacy of Participant Information Storage*

1. Participant information collected is kept in an individual participant record.
2. Each participant record has a unique identification number
3. A participant record includes: personal information • clinical notes • investigations • correspondence from other healthcare providers • photographs • video footage.
4. Child and Adolescent uses an information storage program, sync, that includes password protection, certified security and expiry dates. Only authorised staff will have access to this program and documents will only be available to those necessary. Expiry dates allow Child and Adolescent Psychology to provide access to information for a limited amount to ensure that participants information is safe. of time Other security related procedures such as user access passwords, multi-factorial authentication also assist with the protection of information.
5. Paper records are kept in locked, fireproof cabinets.
6. Participant information is stored for seven years post the date of last discharge. In the case of participants aged under 18 years, information is kept until their 25th birthday and 7 years post discharge.
7. Participant related information, or any papers identifying a participant are destroyed by shredding and deleting from the computer and all databases.
8. User access to all computers and mobile devices holding participant information is managed by passwords and automatic inactive logouts.

*Archiving and storing information*

When records are no longer active, they will be kept in a separate folder and archives for the appropriate time, as dictated by legislative requirements at the time.

Records will be archived in a manner that allows for easy access.

Hardcopy documents will be stored in a locked filing cabinet, located in an environment that reduces the risk of moisture or fire damage.

*Managing Privacy and Confidentiality Requirements of Participants*

1. Child and Adolescent Psychology Services refers to their Privacy Policy on the participant’s NDIS Service Agreement.
2. The NDIS Service Agreement includes 5 Consents:
3. Consent for sharing and obtaining Information
4. Consent for receiving services
5. Consent for photography
6. Consent to participate in Participant Satisfaction Surveys
7. Consent to participate in Quality Management Activities

These consents are discussed with the participant and /or their decision maker in a way they can understand prior to the commencement of service.

1. Persons contacting Child and Adolescent Psychology Services with an enquiry do not need to provide personal details. However, once a decision is made to progress to utilising Child and Adolescent Psychology Services’ services, personal and sensitive information will need to be collected.
2. Child and Adolescent Psychology Services may need to share pertinent participant information with other professional Allied Health Professional at the time of case conferencing or when determining support plans. Information is only shared to provide the best service possible and is only shared with those people whose Professional Codes of Ethics include privacy and confidentiality. Permission to share information is sought from the participant prior to the delivery of services and as required at other points of intervention as / if required.
3. Personal information is not disclosed to third parties outside of Child and Adolescent Psychology Services, other than for a purpose made known to the participant and to which they have consented, or unless required by law.
4. Participants are informed there may be circumstances when the law requires Child and Adolescent Psychology Services to share information without their consent.

*Keeping Accurate Participant Information*

Participants are informed of the need to provide us with up to date, accurate and complete information.

Child and Adolescent Psychology Services’ staff update information on the participant record at the time of reviews or when they become aware of change in information.

AHP staff at Child and Adolescent Psychology Services update the participant record as soon as practical after the delivery of services to ensure information is accurate and correct.

Non-current information will be taken off the participants active files and transferred into a folder for secure storage and possible future reference.

Managers will:

* Ensure files are up to date
* Ensure forms are completed properly
* Ensure non-current information has been archived
* Ensure progress notes have been complete and are accurate

*Using Participant Information for Other Purposes*

Under no circumstances will Child and Adolescent Psychology Services use personal details for purposes other than stated above, unless specific written consent is given by the participant or their representative.

*Participant Access to Their Information*

Participants have the right to access the personal information Child and Adolescent Psychology Services holds about them. To do this, participants must contact the Director of Child and Adolescent Psychology Services.

*Staff records*

Staff files are kept on Sync or in a locked filing cabinet. Staff files are only available to authorised management and the CEO. The staff member can access their file upon request.

*Meeting minutes*

Meeting minutes are to be typed and uploaded to sync.

*Electronic information management*

Data Storage:

* All data if stored on Sync
* Managers and the CEO are the only ones able to add new documents

Backup:

* Sync is a cloud-based program and therefor doesn’t need to be manual backed up

Log-in:

* Each relevant staff member is assigned their own log-in by the CEO

Email:

* Staff should restrict the number of personal emails they receive through their work address
* All inappropriate emails and spam emails should be deleted and opened under no circumstances

Support

* If staff are unable to resolve an IT issue, then arrangements for an IT consultant to assist will be made

Social media:

* Any information that employees share on social media must ensure the privacy and confidentiality of Child and Adolescent Psychology Services and the participants
* Staff must not post any images or information regarding participants
* Staff cannot share any information regarding their work on social media
* If staff are confused about the appropriateness of sharing information related to their work, they should contact management for guidance

*Management of a Privacy Complaint*

1. If a person has a complaint regarding the way in which their personal information is being handled by Child and Adolescent Psychology Services, in the first instance they are to contact the Director. The complaint will be dealt with as per *the Complaints Management Policy*. If the parties are unable to reach a satisfactory solution through negotiation, the person may request an independent person (such as the [Office of the Australian Privacy Commissioner](https://www.oaic.gov.au/privacy/privacy-in-your-state/)) or the [NDIS Quality and Safeguards Commission](https://www.ndiscommission.gov.au/providers/ndis-code-conduct) to investigate the complaint. Child and Adolescent Psychology Services will provide every cooperation with this process.

**Appendix 1: Summary of the 13 Australian Privacy Principles**

**APP 1 — Open and transparent management of personal information**

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

**APP 2 — Anonymity and pseudonymity**

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

**APP 3 — Collection of solicited personal information**

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of ‘sensitive’ information.

**APP 4 — Dealing with unsolicited personal information**

Outlines how APP entities must deal with unsolicited personal information.

**APP 5 — Notification of the collection of personal information**

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

**APP 6 — Use or disclosure of personal information**

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

**APP 7 — Direct marketing**

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

**APP 8 — Cross-border disclosure of personal information**

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

**APP 9 — Adoption, use or disclosure of government related identifiers**

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

**APP 10 — Quality of personal information**

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

**APP 11 — Security of personal information**

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

**APP 12 — Access to personal information**

Outlines an APP entity’s obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

**APP 13 — Correction of personal information**

Outlines an APP entity’s obligations in relation to correcting the personal information it holds about individuals.