Advocacy for Disability Access and Inclusion Inc.

Policy & Procedure

Privacy and Confidentiality

Policy

Purpose

This policy governs the way ADAI deals with personal and sensitive information. We treat personal and sensitive information in a way that is lawful, fair and not unreasonably intrusive to your privacy. Our Privacy Policy is in line with the Australian Privacy Principles listed in the Privacy Act 1988.

Scope

This policy applies to all ADAI permanent, casual, contract, and service staff, volunteers, visitors, contractors and other persons whilst on the organisation's premises or other sites where work is being performed. For this document, the term "Personal information" has the same meaning as in the Privacy Act. Personal information is any information that can be used to personally identify you, including your name, address, phone number, email address and profession or occupation. The term "Sensitive information" means health, racial background, religious or political beliefs or date of birth.

Principles

Each person who contacts ADAI has a right to expect to have the information they provide to the organisation to be kept strictly confidential. Our policy helps us to build trust and confidence in our services. It covers:

- the kinds of personal information that we collect and hold, how we use, store and disclose that information.
- how we will keep your personal information confidential and respect the boundaries of our role. Our authority of access and use extends only to situations where we have an obligation to access or use your information.
- things we won't do, like ask for information we don't need or use information gained from a third party about you without written consent.
- how you:
  - can choose to remain anonymous or use a pseudonym and the consequences of that choice,
  - can request access or correct the information we hold about you, and
  - can complain if you think we have breached our policy.
- our commitment to review our policy to make sure it stays relevant.

ADAI's adherence to the Australian Privacy Principles

Open and transparent management

We publish our privacy policy on our website and regularly review the policy as part of our commitment to continuous improvement and transparency.

Anonymity and pseudonymity

We allow you to deal with us anonymously wherever possible, and this choice may limit the services you are able to access from us.

Using personal information

We collect personal information only to carry out our business, deliver our services and for continuous improvement. We don't usually collect sensitive information but if it is essential for our service delivery, we will ask you for your permission first.

Unsolicited personal information

We do not ask for information we don't need. If you give us personal or sensitive information, we don't store it and/or we securely destroy it.

How and why we collect personal information

We collect personal information from you during normal service delivery, such as when we respond to your enquiries, when we email you and talk to you on the phone or market our services to you. We will also collect information when you become a member, an employee, participate in our surveys or access and use our website.

We usually collect personal information directly from you. However, if your personal information is given by a third party, we require written confirmation that they have a legal right to give it, and that we have the right to use it.

Personal information is used by us to conduct administrative and deliver services including:

- managing and maintaining our business relationships
- providing and improving our services, informing you about our services and obtaining your feedback about them
- sending communications, responding to enquiries and requests and giving you a more personalised experience when you interact with us
- updating our records and keeping contact details up to date, enabling you to subscribe to our website, newsletters and mailing lists and register for our events
- complying with legal requirements and processing and responding to privacy complaints

We will only collect information we need to conduct our business and maintain our relationship with you. We will not share, sell, rent or disclose your personal information other than as described in this policy.

Disclosure of personal information

We may disclose your personal information to our employees and related organisations for our purposes listed above.

Your data will not be made available to a third party, without your consent, unless it is legally required and verified. If we have information that should be communicated to a third party in order to limit or prevent adverse consequences for a client and/or other employees we have an obligation to share information with those who need to know. In these instances, the information is limited to minimum operational facts and avoids the release of personal information as far as practicable.

Except as set out above, we will only disclose personal information if it is required by law or a court or tribunal order or is otherwise permitted under the Privacy Act.

Under the Australian Privacy Act 1988 (Privacy Act) and Privacy Amendment (Notifiable Data Breaches) Act 2017, ADAI will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) if a data breach has occurred and is likely to result in serious harm to individuals whose personal information is involved.

Direct Marketing

We may send you marketing communications to tell you about our services, our surveys or something we think will interest you. We may send communications in various forms, including SMS and email, in line with your consent and relevant laws, such as the Spam Act 2003. If you tell us you prefer a certain method of communication, we will take reasonable steps to use that method whenever it is practical to do so. If you do not want to receive communications from us, you can opt out. You can either use the opt-out method provided in our communications or contact us directly. We will then remove your name from our mailing list. We do not provide your personal information to other organisations for the purposes of direct marketing.

Cross-border disclosure of personal information

We will not disclose your personal information to any other organisation, nor will we send any information overseas for any purpose whatsoever.

Use of government related identifiers

We will never adopt your government identification number to identify you. We may assign our own identification number to protect the confidentiality of your personal information.

Keeping your personal information up to date

We will take all reasonable steps to ensure that the personal information we hold about you is accurate, up to date and complete. We may contact you from time to time to check we have the right information.

How we secure your personal information

We take all reasonable precautions to ensure that personal information is protected from misuse, interference, loss, unauthorised access, modification or disclosure. To do this, we use a combination of physical, administrative and technical safeguards. Our staff are contractually bound by confidentiality obligations. We hold your personal information in either paper-based records in a secure, access-controlled premises or electronic form in databases and email files which require logins and passwords.

How you can access your personal information

At any time, you can ask to access the personal information we hold about you. If you wish to access your personal information, write to our Chief Executive using the contact details provided on our website. We will respond to you within 30 days of receiving your request. If we deny your request, we will provide you with our reasons in writing. We will also tell you how you can complain about our refusal.

Correction of personal information

You can also ask us to correct your personal information if it is inaccurate, incomplete or out of date. We will meet your request where it is reasonable and practicable to do so. However, we may deny access as permitted by the Privacy Act. For example, we may need to refuse access if doing so would interfere with others' privacy, is unlawful or would result in a breach of confidentiality.

Responsibilities

Board

- Regularly review this policy, related systems and the wider legal and/or regulatory environment to ensure this policy is adequate, especially after any data breach.
- Ensure appropriate resources are available to meet the legislative requirements and to uphold the Australian Privacy Principles.

Chief Executive

- Develop, implement and ensure compliance with privacy and confidentiality policy and procedures.

- Allocate resources to appropriate systems to meet policy requirements.
- Ensure Position Descriptions stipulate the level of access to clients' personal information.
- Ensure that staff and volunteers understand their obligations under this policy.

Staff

- Comply with ADAI policies and procedures for privacy and confidentiality.
- Ensure they have the necessary authority and delegation to access and release personal information.

Storage and Record Keeping

This document is stored on the ADAI Corporate Drive.

Related Policies & Procedures

- Code of Ethical Conduct
- Consumer
- Advocacy
- Records Management
- Harm Prevention

Related Standards and Legislations

- Australian Privacy Principles as outlined in the Privacy Act 1988 (Cth),
- Office of the Australian Information Commissioner (OAIC) Ph: 1300 363 992
- Privacy Guidelines for Organisations (OAIC)
- Privacy Amendment (Notifiable Data Breaches) Act, 2017, (Cth)
- Privacy Amendment (Private Sector) Act 2000, (Cth)
- Disability Services Act 1986, (Cth)
- Disability Services Act 1993, (SA)

Review

Frequency	Biennial	**Administrator**	CEO
Next review date	April 2026	**Custodian**	Board

Version Control

Version number	3.0	**Policy No.**	11
Nature of Revision	New template	**Author**	CEO
Approval date	April 2024	**Approved by**	Board

Procedure

Personal Information

Client case discussions are to be conducted confidentially. Client consent is required to have a case discussed with workers from other agencies. Consent may be verbal or written and verbal and must be noted in the client's file.

No personal information about a client, their family, and employee or circumstances can be released to anyone outside of ADAI unless it is a requirement as part of a staff member's official duties. Information provided must be accurate, relevant, fair, current, and non-judgemental.

Case Files

Confidential emails and faxes must state the legal responsibility of the sender and recipient and must be stored on case files. Confidential faxes must be sent/received with a preceding phone call to confirm confidentiality of the document can be maintained.

Client files will be stored securely and will only be accessed on a need to know basis by authorised staff. Files will be identified by number. Documents from clients are kept on file only as long as needed and then returned to the client.

Such files and information remain the property of ADAI and must not be copied or removed unless as a result of a court order or authorised by the Chief Executive.

Case files may only to be removed from the ADAI office if:

- The file is closed and will be archived at Head Office.
- An advocate has permission to work at home in special circumstances (incapacity, office site renovation etc.).
- It is essential for an advocate to have immediate access to the complete file, regardless of location, i.e. Negotiated Education Plans, home visits. In this situation, the strict confidentiality of the file must be maintained.

Data Breach Response Plan

In the event of a data breach per the Privacy Amendment (Notifiable Data Breaches) Act 2017, the Chief Executive Officer is the appointed responsible person.

As the appointed responsible person the Chief Executive will conduct a quick assessment of a suspected eligible data breach to determine whether it is likely to result in serious harm deemed as a notifiable breach.

An eligible data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Where it is likely to result in serious harm, the responsible person must notify the individual or individuals whose

personal information is involved in the data breach, and the Office of the Australian Information Commissioner.

The notification must include a description of the eligible data breach, the kinds of information involved, and what steps the entity recommends that individuals at risk of serious harm take in response to the eligible data breach. Notifications to the Commissioner must be submitted online via the Office of the Australian Information Commissioner https://www.oaic.gov.au/

The Board, in collaboration with the Chief Executive and staff will also conduct a review of its privacy and confidentiality processes and make any necessary amendments to minimise any further risk of data breaches.

Storage and Record Keeping

This document is stored on the ADAI Corporate Drive.

Related Policies & Procedures

- Code of Ethical Conduct
- Consumer
- Advocacy
- Records Management
- Harm Prevention

Related Standards and Legislations

- Australian Privacy Principles as outlined in the Privacy Act 1988 (Cth),
- Office of the Australian Information Commissioner (OAIC) Ph: 1300 363 992
- Privacy Guidelines for Organisations (OAIC)
- Privacy Amendment (Notifiable Data Breaches) Act, 2017, (Cth)
- Privacy Amendment (Private Sector) Act 2000, (Cth)
- Disability Services Act 1986, (Cth)
- Disability Services Act 1993, (SA)

Review

Frequency	Biennial	**Administrator**	CEO
Next review date	April 2026	**Custodian**	Board

Version Control

Version number	3.0	**Procedure No.**	11
Nature of Revision	New template	**Author**	CEO
Approval date	April 2024	**Approved by**	Board

This procedure is approved by: