

# Privacy Policy



## Our organisation

Access Australia Group's (AAG) management and staff is committed to delivering quality employment services, accredited training, community and social activities and disability services for service participants and employers in Victoria. We are a certified quality assured organisation that is subject to the Australian Privacy Principles contained in the *Privacy Act 1988*. AAG will take all reasonable steps to collect, retain and dispose of all relevant personal and/or sensitive information in a lawful, fair and responsible manner.

## Purpose

The purpose of this policy is to uphold the right to people's privacy and will explain how AAG will comply under the Privacy Act 1988. As an accredited quality assured organisation, AAG will ensure that participants, stakeholders, volunteers and all members of the public who deal with our organisation, are aware of, and understand, our privacy obligations under the Act. Document control systems, such as regular reviews by staff/management will ensure that policies such as this are maintained as part of our internal and external audit reviews. The policy is freely available, and accessible on AAG's website:

[www.accessaustralia.org.au](http://www.accessaustralia.org.au)

Under the Health and Human Services' service agreement, clause 17.3(i), Department of Health and Human Services funded organisations (of which AAG is one) must immediately notify the department when becoming aware of a breach, or possible breach, of the organisation's obligations under the *Privacy and Data Protection Act 2014* or the *Health Records Act 2001*. The purpose of this is to ensure timely and effective management of privacy incidents, and to learn from incidents to improve how client information is handled.

## Regulations

- AAG's Consent form (QF1-001)
- Australian Privacy Principles contained in the Privacy Act 1988 (revised 31 March 2015)
- Disability Services Act (1986) (Cth)
- Freedom of Information Act 1982 (Cth)
- Health Records Act 2001 (Vic)
- Information Privacy Act 2000 (Vic)
- Intellectual Property Policy (QPOL1-032)
- National Standards for Disability Services
- Privacy Act 1988 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Public Records Act 1973 (Vic)
- Standards for Registered Training Organisation's (RTOs) 2015 (Cth)

## Definitions

**Australian Privacy Principles (AAP)** - Australian Privacy Principles are contained in the Privacy Act 1988. (see 'Australian Privacy Principles' below for further information.)

The **Australian Privacy Principles guidelines** outline: the mandatory requirements in the APPs, which are set out in Schedule 1 of the Privacy Act; the Information Commissioner's interpretation of the APPs, including the matters that the Office of the Australian Information Commissioner may take into account when exercising functions and powers relating to the APPs; examples that explain how the APPs may apply to particular circumstances; good privacy practice to supplement minimum compliance with the mandatory requirements in the APPs.

**Consent** - means 'express consent or implied consent'. The four key elements of consent are: 1) the individual is adequately informed before giving consent; 2) the individual gives consent voluntarily; 3) the consent is current and specific, and 4) the individual has the capacity to understand and communicate their consent.

**Privacy incident** - A privacy incident may be a breach, a possible breach or a 'near miss'.

- **Breach or Possible Breach** – an action or omission that results in loss, theft, misuse or unauthorised disclosure of personal information, or has the potential to do so.
- **Near Miss** – are situations where a breach would have occurred without intervention. This includes situations where a privacy incident has occurred without any actual disclosure of personal information
- Where a complaint has received advising that a privacy breach has occurred, an investigation must be initiated as per the Data Breach Policy.

**Privacy Incident Report Form** - The Privacy Incident Report Form is to be used to notify the Department of privacy breach incidents the form is accessed via the following link -

<https://feedback.dhhs.vic.gov.au/layout.html#/privacy>

**Sensitive information** - is a special category of personal information and has more strict Privacy Law obligations for collection, storage and use. Under the Privacy Laws, information will generally be considered 'sensitive information' where it is personal information more specifically about a person's: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal records. Health information about a person or genetic information or biometric information is also a form of 'sensitive information'. Sensitive information must not be collected unless: the individual specifically consents to the information being collected; and the information is reasonably necessary for one or more of your functions or activities.

## Policy

### Australian Privacy Principles

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* also known as the *Privacy Amendment Act* includes a set of new, harmonised, privacy principles that will regulate the handling of personal information. These new principles are called the Australian Privacy Principles (APP). Under the changes, there are 13 new APPs. AAG details each APP below and how it complies. Personal information held by AAG may include: Employment records; personal details; enrolment records; job search records; educational qualifications; records of complaints and appeals; Working with Children checks; and health records.

#### 1. Open and transparent management of personal information

We are committed to continually improving our provision of a quality service. AAG will only collect information that is directly related to our service provision. As part of our Quality Management

System, we encourage you to let us know if you have any concerns regarding our handling of your personal information. As stated above, our Privacy Policy (QPOL1-008) and the AAG Website Privacy Policy (QPOL10-002) is available on our website and will be updated when necessary. If a participant wishes to express concern or complain about a breach in the managing of personal information, the complaints process is clearly defined and can be followed. The Feedback, Appeals and Complaints Procedure (QP1-001) is accessible on AAG's website. The Privacy Policy (QPOL1-008) is available from the main office of AAG (18-20 St Andrews Avenue, Bendigo), from AAG's websites and is also included in a service participant's introductory handbook. Students are advised about the AAG's Privacy Policy at pre-enrolment sessions.

## **2. Anonymity and pseudonymity**

Services participants and stakeholders can choose to make a general enquiry anonymously or by using a pseudonym. Government contracts and conformity for our employment services and the registered training organisation can make this request quite difficult. For instance, in the large majority of cases, AAG will require personal information from service participants on a daily occurrence.

## **3. Collection of solicited personal information**

Personal information is used for the purpose of providing employment, disability and training services. In order to carry out these services, personal information may also be provided to government departments and agencies for funding, eligibility and mandatory reporting. Other examples of the people or organisations which may provide us with information, with the authorisation of service participants and other stakeholders, includes; past and potential employers; family members; medical practitioners; and service providers. What we collect depends on the type of service you receive; for our job seekers this may include a current resume or a list of qualifications. When AAG is provided with personal information from a third party it is stored in a secure manner, both physically and electronically.

## **4. Dealing with unsolicited personal information**

When AAG receives unsolicited personal information, which we have not sought, we will check the information is relevant and necessary for the service we provide. Such information will be handled in the same way as other personal information collected. If the unsolicited information is not relevant to the service, such information will ultimately be securely disposed of as required by legislation.

## **5. Notification of the collection of personal information**

Personal information is only obtained with the approval and knowledge of the service participant. AAG will not collect sensitive information without your written consent. Service participants, students and other clients of AAG are notified how and why personal information has been collected and its intended use.

## **6. Use and disclosure of personal information**

- i. The use of personal information primarily for marketing purposes will only be available to be used after you have signed the Consent form (QF1-001). Personal information, held by AAG, regarding our services may be observed by our Information Technical Support service providers, quality assurance certification bodies, and registered auditors. When this happens, the personal information will be presented in such a way that the individual shall not be identifiable. Furthermore, AAG will only use a service participant's personal information for which it was collected, for instance, a resumé is used for direct marketing purposes only to potential employers.

- ii. It is expected that you will be able to understand the information provided to you regarding consent but there are issues that could affect your capacity to consent. These issues could include: age; physical or mental disability; temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia; or has a limited understanding of English. Provisions will be made to ensure that you are involved, as far as practicable, in any decision-making process. *(For more information on the decision-making process please refer to AAG's Supported Decision Making and Advocacy Policy - QPOL1-020)* for you could include: this could include; interpreters; guardians, family, etc. A person aged 15 years and older has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. AAG has the right to assess, on an individual basis, whether this is the case. Individuals under the age of 15 are presumed not to have capacity to consent.
- iii. AST will disclose your name and details via the enrolment form only after the privacy section has been read, understood and signed. Victorian Student Numbers, Unique Student Identifiers, and enrolment information will be forwarded to governing and funding bodies through its Student Management System. AST's external auditors will also have access to your personal details. Privacy statements are located in AST's Enrolment form (QF6-003.1) and the AST USI Privacy notice (QF6-007). You are to read and understand the detail before agreeing and signing these forms.

## **7. Direct marketing**

AAG may only disclose personal information for direct marketing purposes if certain conditions are met. For example, as part of the Department of Social Services contract obligations, AAG will directly market service participants for the purposes of employment. A disclosure of information form is signed by the service participant before any such marketing occurs. A service participant can decline direct marketing if he / she has other means of securing employment (i.e. finding own employment).

## **8. Cross-border disclosure of personal information**

AAG will ensure that the disclosure of personal information of service participants is done so with written consent. In considering cross-border disclosures (i.e. overseas disclosure), AAG will ensure that service participants fully understand and consent to the sharing of personal information, such as images or content before information is made available to another country.

## **9. Adoption, use or disclosure of government related identifiers**

The use or disclosure of a government related identifier of an individual will only occur with written consent of the service participant. AAG may be obliged legally to provide personal information with a government organisation, such as a Job Seeker or Student ID numbers including Unique Student Identifier and Victorian Student Number.

## **10. Quality of personal information**

AAG will take all reasonable steps to ensure any personal information collected or disclosed in relation to service participants is accurate, current, relevant and complete.

## **11. Security of personal information**

AAG will take all reasonable steps to protect the personal information it holds. All personal information that it receives is kept in a lockable file that only authorised personnel have access to. All files are locked after hours and the premises are protected by an electronic security monitoring system. All information that is stored electronically is password protected, with access given to

authorised personnel. Disposal of personal information is contained in AAG's 'Archiving, Retrieval and Destruction Procedure' (QP1-000). Access to this procedure is available at the main office of AAG, 18-20 St Andrews Avenue, Bendigo.

## 12. Access to personal information

You are entitled, according to legislation, to access the personal information an organisation holds about you, unless the organisation is not required to do so under clause 12.3 of the Australian Privacy Principles. If you wish to view this information, AAG will make this available for you within 10 (ten) working days. The contact details for AAG's Privacy Officer is: (03) 5445 9800 or [info@aag.org.au](mailto:info@aag.org.au).

If you are a student with AST you will be required to complete the 'Request for Access to Student records' form (QF6-025) which is accessible from the main office of AST - 22 McLaren Street, Bendigo. Should you require copies of any of your personal information, administrative charges may apply

## 13. Correction of personal information

Individuals have the right to request access to their personal information and to request its correction. All reasonable steps will be taken to ensure that correction of personal information is done in a timely manner. It is important that personal information is accurate, up to date, relevant and not misleading. If AAG refuses a service participants' request for the correction of their personal information, AAG's Feedback, Appeals and Complaints Procedure (QP1-001) should be followed and the Feedback, Appeals and Complaints form (QF1-003) should be filled in.

**For more information about the Australian Privacy Principles, please refer to the Privacy fact sheet 17: Australian Privacy Principles:**

[www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles](http://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles)

## Privacy Incident Reporting:

### *Client information*

Funded agencies have access to a client's personal, health and sensitive information, which is often provided on the basis of trust.

It is critical that funded agencies protect the privacy of this information. When a privacy breach, possible breach or near miss has occurred, Funded Agencies must capture this information and report this privacy breach to DHHS.

*Refer to service agreement clause 17.3(i), under the 'Privacy and Data Protection Act 2014' or the 'Health Records Act 2001'.*

### *Reporting privacy breaches alongside CIMS*

Funded organisations previously reported privacy incidents as category one critical incident reports. With the introduction of the Client Incident Management System (CIMS) a new privacy incident report form was developed, a web-based form in the Feedback Management System (FMS), to enable funded organisations to continue notifying the department about privacy incidents.

A privacy breach that impacts a client may need to be reported as a client incident under CIMS as well as through a privacy incident report.

### *Capturing privacy incidents*

The **Privacy Incident Report Form** captures details relating to:

- the privacy incident

- the clients impacted
- the immediate risks
- how the incident is being managed and if a breach has occurred, how it is being contained
- information relating to security and breaches.

### ***Reporting privacy incidents***

Funded Agencies must report all client related privacy incidents to the department within one business day of becoming aware of, or being notified of a possible privacy incident, or within one business day of an allegation being made of a potential breach.

Possible privacy breaches should continue to be reported on, as well as confirmed breaches

### ***Purpose of notifying DHHS***

The purpose of notifying privacy breaches allows the department to:

- ensure timely and effective management of privacy incidents
- follow up with clients/ service user in a timely and respectful manner
- address contributing factors and develop actions to prevent future privacy breaches
- assist in identifying systemic issues
- learn from incidents to improve how client information is handled.