

# Privacy Policy and Procedure

---

## Contents

1	Purpose and Scope .....	2
2	The Policy.....	2
3	Implementation .....	2
4	Procedure/s .....	2
4.1	Open and Transparent Management of Personal Information.....	2
4.1.1	Types of Personal Information.....	3
4.2	Collection of Personal Information .....	4
4.2.1	Purpose of Collecting Personal Information .....	4
4.2.2	Manner of Collecting Personal Information .....	5
4.2.3	Personal Information of Overseas Learners .....	5
4.3	Dealing with Personal Information.....	5
4.3.1	Use and Disclosure of Personal Information .....	5
4.3.2	Direct Marketing .....	6
4.3.3	Cross-Border Disclosure of Personal Information.....	6
4.3.4	For CRICOS Providers or Providers Conducting Training and Assessment Offshore .....	7
4.3.4.1	Adoption, Use or Disclosure of Government Related Identifiers .....	7
4.4	Integrity of Personal Information.....	7
4.4.1	Quality of Personal Information .....	7
4.4.2	Security of Personal Information .....	8
4.5	Access to and Correction of Personal Information .....	8
4.5.1	Exception to Access.....	8
4.5.2	Dealing with Requests to Access.....	9
4.5.2.1	Other Means of Access .....	9
4.5.3	Access Charges.....	9
4.5.4	Refusal to Give Access.....	9
4.5.5	Correction of Personal Information .....	10
4.5.6	Refusal to Correct Information .....	10
5	Definitions.....	10
6	Related Documents .....	11
7	Review .....	12
8	Revision History .....	13

## 1 Purpose and Scope

This policy ensures that AIE complies with its privacy obligations towards learners and employees.

This policy applies to the entire operations of AIE.

## 2 The Policy

It is a legislative requirement that client privacy be maintained at all times. In addition, AIE respects the privacy of staff and students and always strives to achieve the highest possible level of privacy protection.

In Australia, privacy law generally relates to the protection of an individual's personal information. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

The *Privacy Act 1988* (Cth) includes 13 [Australian Privacy Principles \(APPs\)](#). The APPs set out standards, rights and obligations for the handling, holding, accessing and correction of personal information (including sensitive information).

Private schools and private tertiary educational institutions are required to abide by Australia's privacy legislation.

This policy is based on the 13 APPs that came into force on 12 March 2014 through the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) and details how AIE complies with each of the APPs.

## 3 Implementation

The CEO is responsible for the approval of this policy after it has been drafted or reviewed by Human Resources.

The policy is to be implemented via induction and training of staff and distribution via the AIE intranet and other publications as required.

## 4 Procedure/s

### 4.1 Open and Transparent Management of Personal Information

The Chief Executive Officer of AIE (or Delegate) must:

- a. Ensure the personal information AIE collects is managed openly and transparently
- b. Take reasonable steps to implement practices, procedures and systems to respond to enquiries or complaints about AIE's compliance with the Australian Privacy Principles
- c. Ensure that AIE has a clearly expressed and up-to-date policy about the management of personal information by AIE
- d. Ensure that AIE's *Privacy Policy and Procedure* contains the following information:
  - I. The kinds of information that AIE collects and holds
  - II. How AIE collects and holds personal information
  - III. The purposes for which AIE collects, holds, uses and discloses personal information
  - IV. How an individual may access personal information about the individual that is held by AIE and seek correction of such information

- V. How the individual may make a complaint about a breach of the APPs and how AIE will deal with such a complaint
  - VI. Whether AIE is likely to disclose information to overseas recipients
  - VII. If AIE is likely to disclose information to overseas recipients – the countries in which such recipients are likely to be located (if it is practicable to specify those countries in the policy)
- e. Ensure this *Privacy Policy and Procedure* must be available free of charge and in such form as appropriate
  - f. Must take reasonable steps to make this *Privacy Policy and Procedure* available in a format requested by a particular individual or body.

Individuals may make a complaint about how AIE collects, uses, holds or discloses personal information or breaches this policy by contacting AIE directly following AIE's formal complaints and appeals process. Alternatively, individuals may contact the [Office of the Australian Information Commissioner](#) on the details listed at the end of this policy.

#### 4.1.1 Types of Personal Information

AIE collects, holds and uses the following personal information:

- a. Information required for completion of [Australian Vocational Education and Training Management Information Standards System \(AVETMISS\)](#) data, including, but not limited to name, address, prior education, etc.
- b. Copies of photographic personal identification, relevant qualifications and certificates to assist AIE to determine eligibility for study or employment at AIE
- c. For some courses that are undertaken through or in conjunction with government funding, any government requirements for assessing eligibility, including, but not limited to, concession details and job seeker identification details
- d. Training contracts signed by multiple parties where a client enrolls in a course under a training contract
- e. Academic progress results, including any feedback that may support the student in improved performance
- f. Attendance records, including the dates and times of student attendance
- g. Some courses may require the collection and holding of health and medical information
- h. Student support information, including confidential notes from meetings with relevant stakeholders, that is collected to assist the student with achieving satisfactory course progress. This information is securely stored if collected and held. Any electronic records are securely and confidentially stored within the confidential notes section of the student management system
- i. Personal contact and identification details, emergency contact details and next of kin details (where these differ)
- j. Complaints and appeals information where a complaint or appeal has been lodged
- k. Language, literacy and numeracy assessments.

Other information that may or may not be collected includes:

- a. Passport information
- b. Visa related information

- c. For individuals with certain payment arrangements, AIE may collect, hold and use banking details as per authorisation
- d. Medical certificates, police reports, psychologist reports or other welfare related documents to support claims of compassionate and compelling circumstances
- e. Police clearances
- f. Working with Children Checks
- g. Permits, licenses, professional endorsements or membership details.

Other forms of data that may be collected, held and used in collaboration with government departments on a regular basis, including via personal identification numbers, include:

- a. Training contracts
- b. Training plans
- c. Work Based Training Agreements
- d. Supervision Records
- e. Competency Logs
- f. [Unique Student Identifier \(USI\)](#) upon implementation
- g. [Victorian Training Guarantee \(VTG\)](#) Number.

Any information that is collected, held and used by AIE is subject to this policy. Where required, this policy will be updated to include any changes to the types of information that are collected, held or used by AIE.

## 4.2 Collection of Personal Information

### 4.2.1 Purpose of Collecting Personal Information

AIE collects, holds and uses the previously mentioned personal information and records:

- a. To assess an applicant's application for:
  - I. Employment
  - II. Enrolment
  - III. Appeal
  - IV. Suspension or deferral of enrolment
- b. To monitor student progress and wellbeing throughout the duration of their enrolment
- c. To monitor employee performance and wellbeing throughout the duration of their employment at AIE. For the purposes of this policy, the term 'employee' includes contractors who are engaged by the company in any capacity
- d. For the purposes of identification of employees to the executive and relevant (or prospective) clients of AIE
- e. For the purposes of submitting the required registration and enrolment records to government authorities for:
  - I. Nationally recognised training requirements (e.g. competency completion data)
  - II. For those courses that are associated with government contracts, to provide information to the relevant State/Territory Training Authority as required by AIE's registration requirements
  - III. External and internal auditing purposes

- f. For financial data, the information is collected and stored for the purpose of facilitating payment in accordance with training contracts and course agreements
- g. To contact the next of kin in the event of an emergency.

#### 4.2.2 Manner of Collecting Personal Information

AIE only collects information as and when required by requesting it to be submitted by the individual with their written consent (this consent may be in the form of an application for enrolment or employment). Information can be collected by AIE through:

- a. Hardcopy submission
- b. Electronic submission via:
  - I. Email
  - II. AIE website including social media sites
- c. Promotions, Open Days and exhibitions.

In the event of an individual having a medical illness or disability, any sensitive medical information is collected, held and used for the purpose of ensuring the safety of self and others.

In the event that AIE is no longer able to operate as a Registered Training Organisation, it will be required to disclose personal information (and potentially sensitive personal information) to other entities where required; however, this would only be undertaken with the client's written consent.

#### 4.2.3 Personal Information of Overseas Learners

AIE is a [CRICOS](#) (Commonwealth Register of Institutions and Courses for Overseas Students) registered provider. As such, AIE also collects, holds, uses and discloses personal information and sensitive personal information to government authorities where required under the [Education for Overseas Students \(ESOS\)](#) legislative framework. These authorities include the Department of Education and Training (DET) and the Department of Immigration and Border Protection (DIBP). In certain other circumstances, AIE may also be required to collect, hold, use and disclose other personal information and sensitive personal information. This includes, for example, homestay applications, information about parents and guardians where the client meets the definition under Standard 5 of the *National Code of Practice for Providers of Education and Training for Overseas Students 2018 (National Code)*. Other special circumstances which might require AIE to collect, hold, use and disclose personal information or sensitive personal information may be in relation to compassionate and compelling circumstances requiring internal or external support, although this will always be undertaken with the client's written consent.

### 4.3 Dealing with Personal Information

#### 4.3.1 Use and Disclosure of Personal Information

AIE will not use or disclose personal or sensitive information for any purpose other than for that which it was collected, unless the relevant person has provided written consent to use or disclose the information in circumstances that are different to those for which it was collected. The circumstances where there may be an exception to this are:

- a. Where the use or disclosure of this information is required or authorised by or under an Australian law or a court/tribunal order

- b. The individual would reasonably expect AIE to use or disclose the information for the secondary purpose
- c. A permitted general situation exists regarding the use or disclosure of the information by AIE
- d. A permitted health situation exists regarding the use or disclosure of the information by AIE
- e. AIE reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by or on behalf of, an enforcement body. Where AIE uses an individual's personal information under this clause, AIE must obtain consent in writing to release, use or disclose the personal information.

Where the individual chooses to maintain anonymity, or use a pseudonym and this is not detrimental to their enrolment or employment (as relevant) at AIE and it does not inhibit AIE's adherence to registration requirements and legislation compliance, AIE will act upon the individual's request as is reasonable in relation to the requested and particular matter.

Where an individual seeks to obtain access to or correction of personal information that is held by AIE, they may do so by written request.

#### 4.3.2 Direct Marketing

Where AIE holds personal information, and excluding any sensitive information about an individual, AIE will not use or disclose this information for the purpose of direct marketing unless the following circumstances apply:

- a. Written consent has been collected by the individual
- b. The individual would reasonably expect AIE to use or disclose the information for that purpose; for example staff identification photos may be used by the executive to identify to clients' (or prospective clients) relevant staff
- c. AIE provides an opt-out method that is easily accessible for individuals to request not to receive direct marketing communications from AIE
- d. The individual has not made such a request to AIE.

Where AIE does have written consent for the collection, holding and use of their personal details (excluding sensitive information), AIE must provide a simple means by which the individual can easily request not to receive direct marketing communications from AIE.

This policy is also supported by and does not replace or supersede the following legislation:

- a. *Do Not Call Register Act 2006* (Cth)
- b. *Spam Act 2003* (Cth)
- c. Any other legislative document of the Commonwealth Government.

#### 4.3.3 Cross-Border Disclosure of Personal Information

Before AIE discloses personal information about an individual to a person who is an overseas recipient and who is not the individual or AIE, AIE must take such steps to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information. This does not apply if the recipient of the information is:

- a. Subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APP's protect the information

- b. There are mechanisms that the individual can access to take action to enforce the protection of the law or binding scheme or both of the following apply:
  - I. AIE expressly informs the individual that if they consent to the disclosure of the information, the above clauses will not apply
  - II. After being so informed, the individual consents to the disclosure
- c. Any of the reasons that apply for exemption under 4.3 Dealing with Personal Information previously.

#### 4.3.4 For CRICOS Providers or Providers Conducting Training and Assessment Offshore

AIE provides nationally recognised training and assessment to clients whose country of origin may be overseas and where an overseas recipient assists them with any of the documentation listed under the heading 'Purpose of Collecting Personal Information'. Further, for clients who are applying for visas based on their proposed enrolment in training and assessment activities at AIE, AIE may be required to disclose certain personal information to AIE agents and representatives, family members of clients and/or government or other enforcement authorities (e.g. Department of Immigration and Border Protection) in those countries or wherever the individual requires AIE to liaise with other entities. Where this is required, the client will provide written consent for this to occur through their enrolment documentation.

##### 4.3.4.1 Adoption, Use or Disclosure of Government Related Identifiers

AIE must not adopt a government related identifier of an individual as its own identifier of the individual unless:

- a. The adoption of the government related identifier is required or authorised by or under Australian law or a court/tribunal order
- b. The identifier is prescribed by the regulations and the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

At AIE, such government identifiers would include (but are not limited to):

- a. Training Contracts
- b. Unique Student Identifier (USI)
- c. Victorian Student Number (VSN)
- d. Job Seeker Identification numbers
- e. Centrelink or other concessional identifiers.

AIE must not use or disclose a government related identifier of an individual unless it is in the circumstances described under the exceptions of 4.3 Dealing with Personal Information previously.

## 4.4 Integrity of Personal Information

### 4.4.1 Quality of Personal Information

AIE must take steps to ensure that the personal information that it collects is accurate, up to date and complete. AIE must take steps (as are reasonable in the circumstances) to ensure that the personal information that AIE uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant. In all cases at AIE, this includes all hardcopy and electronic records.

#### 4.4.2 Security of Personal Information

AIE must take steps that are reasonable in the circumstances to protect the information from misuse, interference and loss as well as unauthorised access, modification or disclosure. AIE achieves this by ensuring:

- a. Any hardcopy files containing hardcopy personal information is held in a room with a closed, lockable door at all times, including where this information is archived. This would include records such as training records and course progress information, assessment feedback etc. Hardcopy personal information, such as enrolment records containing AVETMISS data, for example, will be held in a lockable filing cabinet with a sign in and sign out sheet that must be completed each time the personal information is taken out and returned to the filing cabinet
- b. All electronic student records are maintained on a securely hosted website with appropriate intrusion protection and logical system access requiring each user to enter a user name and password for access
- c. All hardcopy sensitive personal information is to be stored in a lockable filing cabinet in the CEO's office or their delegate
- d. All electronic sensitive personal information has enhanced access protection within the electronic student record to prevent misuse, interference, loss, unauthorised access or modification. The login and password details for this additional layer of security must be different to the user's usual login details
- e. Where the user is physically absent from the personal information or sensitive personal information for any period of time, that person must return the personal information or the sensitive personal information to its secure storage area in accordance with these instructions.

AIE will conduct regular audits, either combined with or separate to its internal audits for registration purposes to confirm compliance with this policy and the Australian Privacy Principles.

AIE must take reasonable steps to destroy and individual's personal information or ensure the information is de-identified if:

- a. The information is no longer needed for the purpose/s for which it was collected
- b. The information is not contained in a Commonwealth record
- c. AIE is not required by or under an Australian law, or court/tribunal order, to retain the information.

Various legislative and registration requirements mean that AIE is required to maintain all enrolment records, including training plans, for 30 years. All training and assessment items are required to be maintained according to the *Student Document Retention and Credentials Policy and Procedure*.

#### 4.5 Access to and Correction of Personal Information

If AIE holds personal information about an individual, AIE must, upon request by the individual, give the individual access to the requested information.

##### 4.5.1 Exception to Access

AIE is not required to give the individual access to the personal information if:

- a. AIE reasonably believes that giving access would pose a serious threat to the life, health or safety of an individual, or to public health or public safety
- b. Giving access would have an unreasonable impact on the privacy of other individuals
- c. The request for access is vexatious or frivolous
- d. The information relates to existing or anticipated legal proceedings between AIE and the individual and would not be accessible by the process of discovery in those proceedings
- e. Giving access would reveal the intentions of AIE in relation to negotiations with the individual in such a way as to prejudice those negotiations
- f. Giving access would be unlawful
- g. Denying access is required or authorised by or under Australian law or a court/tribunal order
- h. Both of the following apply:
  - I. AIE has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to AIE's functions or activities has been, is being or may be engaged in
  - II. Giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- i. Giving access would likely prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body
- j. Giving access would reveal evaluative information generated within AIE in connection with a commercially sensitive decision-making process.

#### 4.5.2 Dealing with Requests to Access

AIE must respond to the request within a reasonable period after the request is made and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

##### 4.5.2.1 Other Means of Access

AIE may refuse to give access due to reasons previously outlined or because the manner requested by the individual is problematic. In these cases, access may be given through the use of a mutually agreed intermediary.

#### 4.5.3 Access Charges

Where AIE is an organisation, AIE may charge for giving access to the personal information; however, the charge must not be excessive and must not apply to the making of the request.

#### 4.5.4 Refusal to Give Access

If AIE refuses to give access to personal information because of any of the reasons previously outlined, or where AIE refuses to give access in the manner requested by the individual, AIE must give the individual a written notice that sets out:

- a. The reasons for the refusal, except to the extent that it would be unreasonable to do so
- b. The mechanisms available to complain about the refusal
- c. Any other matter prescribed by the regulations.

If AIE refuses to give access to the personal information it would reveal information about a commercially sensitive decision-making process, the reasons for the refusal may include an explanation for the commercially sensitive decision.

#### 4.5.5 Correction of Personal Information

AIE must take reasonable steps to correct personal information when:

- a. It is inaccurate, incomplete, irrelevant or misleading
- b. The individual requests that AIE correct the information.

Such corrections should be made in line with the purposes for which the information was collected, and must be accurate, up to date, complete, relevant and not misleading.

#### 4.5.6 Refusal to Correct Information

If AIE refuses to correct personal information (including a request to associate a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading) as requested by the individual, AIE must give the individual a written notice that explains:

- a. The reasons for the refusal, unless it would be unreasonable to do so
- b. The mechanisms available to complain about the refusal
- c. Any other matter prescribed by the regulations.

Where AIE is required to provide a statement, AIE must take steps that are reasonable in the circumstances to associate a statement in such a way that will make the statement apparent to users of that information.

AIE will endeavour respond within 30 days after the request is made. AIE will issue a statement within a reasonable period after the request is made and will not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

For further questions or clarity regarding the *Privacy Act 1988* (Cth), please contact the Office of the Australian Information Commissioner as detailed below:

- Telephone:** 1300 363 992  
**Mail:** GPO Box 5218  
Sydney NSW 2001  
**Email:** [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)  
**Website:** <http://www.oaic.gov.au>

## 5 Definitions

### **Australia Vocational Education and Training Management Information Statistical Standard (AVETMISS)**

The national data standard that ensures consistent and accurate capture and reporting of Vocational Education and Training (VET) information about learners. RTOs must comply with AVETMISS reporting requirements. <sup>^</sup>

### **Australian Privacy Principles**

A cornerstone of the Australian privacy protection framework that governs standards, rights and obligations around:

- a. The collection, use and disclosure of personal information
- b. An organisation or agency's governance and accountability

- c. Integrity and correction of personal information
- d. The rights of individuals to access their personal information.

### **Commonwealth Register of Institutions and Courses for Overseas Students (CRICOS)**

The Australian Government register listing all Australian education providers that are approved to teach overseas students and the courses that they offer. [^](#)

### **Education Services for Overseas Students (ESOS)**

The legislative framework governing the delivery of education to international students in Australia on a student visa. It protects and enhances Australia's reputation for quality education, provides tuition protection and supports the integrity of the student visa program. [^](#)

### **Office of the Australian Information Commissioner (OAIC)**

The Australian Government independent regulator for privacy and freedom of information. See the [OAIC website](#) for more information.

### **Personal Information**

Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

### **Privacy Act 1988**

The Privacy Act is Federal legislation that was passed in 1988 that protects the privacy of individuals and regulates the handling of personal information. The Privacy Act includes 13 Australian Privacy Principles.

### **Unique Student Identifier (USI)**

A reference number for learners studying Australian courses so they can track their training records and results. [^](#)

### **Victorian Training Guarantee (VTG)**

Victorian State Government initiative that provides subsidised training for eligible learners in approved course. [^](#)

## **6 Related Documents**

**The following internal documents are related to this policy:**

- a. AIE Learner Handbook
- b. AIE Terms and Conditions of Enrolment (aie.edu.au)
- c. Authority to Release Information Form
- d. HR Data Recording Policy and Procedure
- e. Information Technology Security Policy and Procedure
- f. Personal Information Policy and Procedure
- g. Request for Access to Personal Learner Record and Information Form (aie.edu.au)
- h. Staff Photos Policy and Procedure
- i. Student Document Retention and Credentials Policy and Procedure.

**The following legislation and standards are related to this policy:**

- a. Australian Privacy Principles <[oaic.gov.au](#)>



- b. Australian Privacy Principles Guidelines (oaic.gov.au)
- c. Do Not Call Register Act 2006 (Cth)
- d. Education Services for Overseas Students Act 2000 (ESOS Act) (Cth)
- e. Education Services for Overseas Students Regulations 2019 (Cth)
- f. Freedom of Information Act 1982 (FOI Act) (Cth)
- g. National Code of Practice for Providers of Education and Training for Overseas Students 2018 (National Code)
- h. Privacy Act 1988 (Cth)
- i. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- j. Spam Act 2003 (Cth)
- k. Spam Regulations 2021 (Cth)
- l. Standards for Registered Training Organisations (RTOs) 2015
- m. Student Identifiers Act 2014 (Cth)
- n. Student Identifiers Regulation 2014 (Cth).

## 7 Review

This policy will be reviewed annually by Human Resources.



## 8 Revision History

Version No.	Version Description	Contributor(s)	Approval Authority	Date Revised/ Approved
1.0	First version of document	-	BOD	-
1.1	Style update.	<b>Casey Gregory</b> (Manager, Planning and Implementation)	-	22 May 2017
2.0	Style update, content restructure, content edit, and content additions (definitions and related documents).	<b>Nick Markesinis</b> (Intranet Content Coordinator)	BOD	18 May 2021/ 30 August 2021