Learner Privacy Policy and Procedure

Contents

1. Purpose and Scope

This policy outlines AIE's responsibilities and procedures collection, storing, using, disclosing and destruction of learners' personal information.

The scope of this policy is all staff.

2. The Policy

AIE upholds the Australian Privacy Principles (APPs) and all legislative requirements surrounding learner privacy. All collection, storage, use, disclosure and destruction of personal information is done securely, for the right purpose, and in accordance with all relevant legislation and standards.

3. Implementation

The Board of Directors is responsible for the approval of this policy after it has been drafted or reviewed by the National Compliance Officer.

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. AIE's Responsibilities

4.1.1. Responsibilities Under the Australian Privacy Principles

AIE is responsible for adhering to the Australian Privacy Principles (APPs) as outlined in the *Privacy Act 1988* (Cth). These responsibilities are:

a. **APP 1:** The open and transparent management of personal information
b. **APP 2:** Providing the option for individuals to deal anonymously or by pseudonym with AIE, unless the individual must be identified due to legislative requirements, or it is impractical to deal with the individual if they have not identified themselves
c. **APP 3:** Ensuring that personal information is solicited or collected:
    I. Only for purposes reasonably necessary or directly related to AIE's operations
    II. For sensitive information, only if the individual consents to the information being collected
    III. Only by lawful and fair means, and only directly from the individual
d. **APP 4:** Handling unsolicited personal information appropriately
e. **APP 5:** Ensuring that all learners are informed about certain 'matters' outlined in APP 5.2
f. **APP 6:** Ensuring that personal information is held, used and disclosed legally and appropriately

g. **APP 7:** Ensuring that personal information gathered for direct marketing is used and disclosed appropriately
h. **APP 8:** Ensuring the overseas disclosure of personal information is secure and that the disclosed personal information to an overseas entity will be used with the utmost care
i. **APP 9:** Ensuring any government-related identifiers, such as a unique student identifier (USI), are used appropriately
j. **APP 10:** Ensuring the personal information collected by AIE is of sufficient quality (accurate, up to date, complete and relevant)
k. **APP 11:** Ensuring that personal information is:

    I. Protected with the strongest security possible to prevent misuse; interference; loss; or unauthorised access, modification or disclosure
    II. Destroyed or de-identified when no longer needed and allowed by law to do so

l. **APP 12:** Ensuring that an individual's personal information is accessible to that individual if requested
m. **APP 13:** Ensuring that personal information is corrected when:

    I. AIE is satisfied that the personal information is inaccurate, out of date, incomplete, irrelevant, or misleading
    II. The individual request AIE to correct their personal information.

4.1.2. Responsibilities Under the ESOS Framework

AIE has privacy responsibilities towards international learners through the *Education Services for Overseas Students Act (EOS) 2000* (Cth) and the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*. These responsibilities are:

a. Adhering to the APPs as outlined in Section 4.1.1 and procedures throughout this policy
b. Ensuring all required international learner personal information is supplied to Australian government regulators

    I. Any changes to international learners personal information should be entered into PRISMS within 31 days of the change occurring.

c. Liaising with education agents regarding international learner personal information.

4.2. Open and Transparent Procedures

AIE has published this *Learner Privacy Policy and Procedure* so that learners and other stakeholders can understand how AIE deals with learner personal information. This policy is publicly and freely available as a PDF on the AIE website and on the staff intranet. If an individual or group requests the policy in a particular format, AIE will take reasonable steps to comply with the request.

This policy is regularly reviewed and updated in accordance with the *AIE Policy Framework*. New, approved versions are sent to Marketing to upload to the AIE website and to the Intranet Content Coordinator to upload to the staff intranet.

AIE staff are trained to understand and handle matters involving personal information.

See the APP 1 guidelines for more information on the open and transparent management of personal information.

4.3. Kinds of Personal Information Collected

4.3.1. General Personal Information

AIE collects and holds the following kinds of personal information when needed due to government requirements, course requirements or personal circumstances:

a. Information required for mandatory government reporting
b. Personal contact and identification details; emergency contact details
c. Copies of photographic personal identification, relevant qualifications and certificates to assist AIE to determine eligibility for study or employment at AIE
d. For some courses that are undertaken through or in conjunction with government funding, any government requirements for assessing eligibility
e. Training contracts signed by multiple parties where a client enrols in a course under a training contract
f. Academic progress results
g. Attendance records
h. Learner support information, including language, literacy and numeracy (LLN) assessments, that is collected to assist the learner to achieve satisfactory course progress
i. Complaints/appeals information where a complaint or appeal has been lodged
j. Passport and visa-related information
k. Banking details
l. Permits and licenses
m. Training contract details
n. Training plan details
o. Work-based training agreement details
p. Supervision records
q. Competency logs
r. Unique Student Identifier (USI)
s. Skills First Funding (SFF) Number
t. Intellectual property

4.3.2. Sensitive Information

AIE collects and holds the following kinds of sensitive information when needed due to government requirements, course requirements or personal circumstances:

a. Health and medical information, if required by particular courses
b. Medical certificates, police reports, psychologist reports or other welfare-related documents to support claims of compassionate and compelling circumstances
c. Police clearances and working with children checks
d. Professional endorsements or membership details

e. Racial, ethnic, religious, sexual orientation details when these details are provided by learners as part of a complaint or appeal.

4.4. Purposes for Collecting, Holding and Using Personal Information

AIE collects, holds and uses personal information and records to:

a. Assess a learner for:
    I. Enrolment
    II. Suspension or deferral of enrolment
    III. Complaint or appeal
b. Monitor learner progress and wellbeing throughout their enrolment
c. Submit required registration and enrolment records to government authorities for:
    I. Nationally recognised training requirements; for example, competency completion data
    II. State/Territory-based government contract requirements
    III. External and internal auditing purposes
    IV. Facilitating payments in accordance with training contracts and course agreements
    V. Contacting next of kin during emergencies.

All learner personal information is stored in AIE's student management system (SMS) or in hard copy format for academic management purposes. All prospective learner personal information is stored in HubSpot for marketing purposes.

4.4.1. Direct Marketing

AIE collects personal information to directly market its training products and services. This information is stored in HubSpot.

AIE will not use or disclose personal information for the purpose of direct marketing unless the following circumstances apply:

a. The individual has provided written consent
b. The individual would reasonably expect AIE to use or disclose the information specifically for direct marketing
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.

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

e. *Do Not Call Register Act 2006* (Cth)
f. *Spam Act 2003* (Cth)
g. Any other legislative document of the Commonwealth Government.

> See the APP 7 guidelines for more information about direct marketing.

4.4.2. Overseas Learners

AIE is a CRICOS (Commonwealth Register of Institutions and Courses for Overseas Students) registered provider. This means AIE collects, holds, uses and discloses personal information to government authorities where required under the Education for Overseas Students (ESOS) Framework. These authorities include:

a. The Department of Education, Skills and Employment
b. The Department of Home Affairs
c. The Provider Registration and International Student Management System (PRISMS).

> See the *Education Services for Overseas Students Regulations 2019* (Cth) and the *National Code of Practice for Providers of Education and Training to Overseas Students 2018* for more information on AIE's responsibilities for mandatory reporting of overseas learner data.

4.5. Collecting Personal Information

AIE only collects personal information when required and only by requesting it to be submitted by prospective learners with their written consent. Consent is given via an enrolment form. Personal information related to VETSL applications is given through an Electronic Commonwealth Assistance Form (eCAF).

Information can be collected by AIE through:

a. Hard copy submissions
b. Electronic submissions via email, the AIE website or social media sites
c. Promotions, open days and exhibitions.

> See the APP 3 guidelines for more information on collecting personal information.

4.5.1. Informing/Notifying Prospective Learners

Prior to enrolment, prospective learners are provided with the Terms and Conditions of Enrolment. This outlines AIE's varying requirements for collecting and reporting personal information to the government.

The *Letter of Offer* links to the *Learner Handbook*, which provides further information about data collection, retention and reporting. The *Learner Handbook* and Terms and Conditions of Enrolment, as well as policies and procedures related to public stakeholders, are also freely available on the website in accessible formats.

> See the APP 5 guidelines for more information on notifying learners of the collection of personal information.

4.5.2. Anonymity or Use of a Pseudonym

If a learner chooses to be anonymous, or use a pseudonym, and this is not detrimental to their enrolment or another process at AIE (such as complaints) and it does not inhibit AIE's adherence to registration requirements and legislation compliance, AIE will act upon if it is reasonable to do so.

> See the APP 2 guidelines for more information on anonymity and use of pseudonyms.

4.5.3. Handling Unsolicited Personal Information

Personal information that is not actively and consciously requested by AIE is considered *unsolicited personal information*.

If AIE receives unsolicited personal information, it must promptly determine if the information could have been collected under APP 3 (for the purposes of its operations and with the giver's consent).

If AIE determines that the personal information ***could not have been*** collected under APP 3, it must promptly destroy or de-identify the information if it is lawful and reasonable to do so. **NOTE: It is unlawful to destroy or de-identify unsolicited personal information if the information is contained in a Commonwealth record.**

If AIE determines that the personal information ***could have been*** collected under APP 3, the information should be treated in line with the other procedures in this policy.

> See the APP 4 guidelines for more information on dealing with unsolicited personal information.

4.6. Quality of Personal Information

AIE must ensure the personal information it collects and uses is *accurate*, *up to date*, *complete* and *relevant*. Quality checks are performed at the following points in the information handling process:

a. When the information is collected
b. When the information is used or disclosed.

> See the APP 10 for more information on ensuring the quality of personal information.

4.7. Holding Personal Information

4.7.1. Security

AIE protects personal information through various physical and technological security measures outlined in Table 1.

Table 1: Security measures for hard copy and electronic learner personal information.

	General Personal Information	Sensitive Personal Information
Hard Copy [1]	Stored in a lockable room in lockable filing cabinets. A sign-in and sign-out sheet must be completed each time the personal information is removed and returned to the filing cabinet.	Stored in a lockable filing cabinet in the CEO's office, or their delegate's office. A sign-in and sign-out sheet must be completed each time the sensitive information is removed and returned to the filing cabinet.
Electronic	Stored on a securely hosted website with appropriate intrusion protection and logical system access requiring each user to enter a username and password for access.	Same storage as general personal information, but with enhanced access protection to prevent misuse, interference, loss, unauthorised access or modification. The username and password details for this additional layer of security must be different to the user's usual logins.

[1] *Where the user is physically absent for any length of time from the storage location of hard copy personal information, that person must return the personal information to its secure storage area in accordance with these instructions.*

Personal information that is no longer needed, is not contained in the Commonwealth record and is not required by any law or court/tribunal order to be kept should be destroyed or de-identified. See Section 4.13 Personal Information Retention, Destruction and De-Identification for AIE's procedures.

4.7.1.1. Data Breaches

AIE complies with the Notifiable Data Breaches (NDB) scheme in the event of a data breach that is likely to result in serious harm to any individuals whose personal information is involved in the breach.

Data breach procedures are outlined in *Information Technology Security Policy and Procedure*.

See the APP 11 guidelines for more information on the security of personal information.

4.8. Accessing Personal Information

AIE must, upon a learner's request, give a learner access to their personal information. The request must be actioned within a reasonable period of time. Access must be provided in the manner requested by the learner, if it is reasonable and practicable to do so.

Learners or their authorised delegates can submit a *Access/Correct Personal Information Form*. Campus Administration will action the request within 30 calendar days.

4.8.1. Verifying Identification

AIE must be able to verify the identity of the learner or person authorised on the learner's behalf who is requesting the personal information. A minimum amount of personal information should be collected and/or sighted to confirm identity.

4.8.2. Refusal to Give Access

AIE is not required to grant individuals access to 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 safety
b. Giving access would have an unreasonable impact on the privacy of other individuals
c. The request for access is *frivolous* (without merit) and *vexatious* (a waste of time)
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 likely prejudice any 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.

> See paragraphs 12.33 to 12.62 of the APP 12 guidelines for more detailed information about these reasons for access refusal.

4.8.2.1. Refusal Notification

If access is refused, AIE will give the requesting individual written notice explaining:

a. The reasons for the refusal, except where it would be unreasonable to do so
b. The mechanisms available to complain about the refusal (see Section 4.12 Personal Information Complaints)
c. Any other matter prescribed by the *Privacy Act 1988* (Cth).

4.8.3. Other Means of Access

If requested access is refused, AIE may offer an alternative means by which the information can be provided, such as through a mutually agreed intermediary.

4.9. Correcting Personal Information

AIE must correct personal information when:

a. It is inaccurate, incomplete, irrelevant or misleading
b. A learner or their delegate requests AIE to correct the information.

Personal information should be corrected (or a refusal to correct provided) within 30 calendar days of the request being received.

AIE does not charge a fee for requesting or actioning the correction of personal information.

4.9.1. Correcting at AIE's Initiative

AIE may correct personal information at its own initiative if an internal or external auditing or monitoring mechanism reveals inaccurate, incomplete, irrelevant or misleading data.

4.9.2. Correcting at the Learner's Request

A learner or their delegate should submit a *Access/Correct Personal Information Form*. The following AIE representatives are responsible for making corrections based on the information provided in the form:

a. **Marketing:** For all personal information in HubSpot
b. **Administration:** For personal information stored in all other locations.

AIE actions the request within 30 calendar days from receipt of the form.

4.9.3. Notification of Correction

Once the personal information is corrected, AIE should notify:

a. Other organisations, entities and agencies where the personal information has been previously disclosed so their records can be updated too
b. The learner whose record was corrected, if the learner did not request the correction.

4.9.4. Refusal to Correct Personal Information

AIE can refuse a request to correct personal information if:

a. AIE does not hold the personal information
b. The information is already accurate, up to date, complete, relevant and not misleading
c. The steps necessary to correct the personal information are not reasonable.

4.9.5. Statement of Uncorrected Personal Information

AIE should take reasonable steps to allow for a statement to be associated with the personal information explaining that the data is inaccurate, out of date, incomplete, irrelevant or misleading.

AIE should notify the learner or delegate of their right to have a statement attached to their personal information in lieu of a correction.

4.9.6. Notification of Refusal to Correct Personal Information

If AIE refuses a request to correct personal information, a written notification must be provided to the learner or delegate outlining:

a. The reasons for the refusal (unless it would be unreasonable to do so; for example, when doing so would prejudice a criminal investigation)
b. The mechanisms available to complain about the refusal (see Section 4.11 Personal Information Complaints)
c. Any other matter prescribed by the *Privacy Act 1988* (Cth).

> See the APP 13 guidelines for more information on correcting personal information.

4.10. Disclosure of Personal Information to Overseas Recipients

AIE may need to disclose a learner's personal information to overseas recipients for the purposes for which the information was collected (such as enrolment, support and progression, and so on). In doing so, AIE must first ensure the overseas recipient will handle the learner's personal information in accordance with the APPs. Overseas recipients of personal information can include, but are not limited to, education agents and government departments from the learner's home country.

4.10.1. Education Agents

Education agents assist AIE in recruiting overseas learners, but must sign an *Education Agent Agreement* before they are allowed to perform this service. Once the agreement is signed, they are added to the *International Education Agent Register*, which is maintained by Marketing. AIE regularly checks the integrity of its education agents.

See 4.2.2 of *Privacy Policy and Procedure.*

4.11. Adoption, Use or Disclosure of Government-Related Identifiers

4.11.1. Adoption

AIE must not adopt a learner's government-related identifier (such as a USI) as its own identifier for that learner. Instead, AIE issues learners with a student number (for example, s123456).

4.11.2. Use and Disclosure

AIE may use or disclose a learner's government-related identifier under the following circumstances:

a. If the use or disclosure is reasonably necessary to verify the learner's identity for the purpose of enrolment
b. To fulfil a Commonwealth or State/Territory contract or as required by legislation
c. To lessen or prevent serious threat to life, health or safety
d. In relation to suspected unlawful activity or serious misconduct.

> See the APP 9 guidelines for more information on the adoption, use or disclosure of government-related identifiers.

4.12. Personal Information Complaints

AIE follows the complaints and appeals process in the *Learner Handbook* and in AIE's *Domestic Student Complaints and Appeals Policy and Procedure* and *International Student Complaints and Appeals Policy and Procedure*.

Visit the Federal Register of Legislation to read the latest version of the *Privacy Act 1988* (Cth). Alternatively, visit the Office of the Australian Information Commissioner (OAIC) to read the Australian Privacy Principles and the Australian Privacy Principles Guidelines.

4.13. Personal Information Retention, Destruction and De-Identification

Information on the retention and destruction of learner personal information can be found in:

a. *Information and Records Management Policy and Procedure*
b. *Student Document Retention Policy and Procedure*.

Most personal information is not de-identified because full details are required for regulatory reporting. However, some data, such as tax file numbers and credit card data, is de-identified.

5. Definitions

The following definitions apply to this policy:

Term	Definition
Anonymity	Being unidentifiable and not having personal information collected.
Australian Privacy Principles (APPs)	A set of 13 privacy principles within the Australian privacy protection framework, outlined in the *Privacy Act 1988* (Cth). Read the legal copy of the Australian Privacy Principles or the APP Guidelines on the website of the Office of the Australian Information Commissioner.
Australian Vocational Education and Training Management Statistical Standard (AVETMISS)	The national data standard that ensures consistent and accurate capture and reporting of Vocational Education and Training (VET) information about learners. Registered Training Organisations must comply with AVETMISS reporting requirements.
Commonwealth Record	According to the *Archives Act 1983* (Cth), s 6(1), a Commonwealth record is 'a record that is the property of the Commonwealth or a Commonwealth institution', or a record deemed as such under the *Archives Act 1983* (Cth) or a regulation of that act. Commonwealth records held by AIE cannot be destroyed or de-identified.
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.
De-Identification	Removing or altering identifiable information such as personal identifiers (name, address, date of birth, and so on) or other information (such as details about physical characteristics) so an individual can no longer be identified with that collection of data.

Education Agent	As defined by the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*, an *education agent* is: 'A person or organisation (in or outside Australia) who recruits overseas students and refers them to education providers. In doing so, the education agent may provide education counselling to overseas students as well as marketing and promotion services to education providers. Education agent does not refer to an education institution with whom an Australian provider has an agreement for the provision of education (that is teaching activities).'
Education Services for Overseas Students (ESOS)	The legislative framework governing the delivery of education to international students in Australia on a student visa.
Government-Related Identifier	An identifier with a string or a combination of letters, numbers and/or symbols assigned by a government agency, a State or Territory authority, an agent acting for a government agency, State or Territory, or a contracted service provider for a Commonwealth or State contract. Examples of government-related identifiers are Medicare numbers, USI numbers, Centrelink numbers, and so on.
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	As defined by the *Privacy Act 1988* (Cth), s 6(1), *personal information* is 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in material form or not.'
Provider Registration and International Student Management System (PRISMS)	A data reporting system under the Education Services for Overseas Students (ESOS) framework.
Pseudonymity	Having a name, term or descriptor that is different to an individual's real name, while still collecting other personal information about them.
Sensitive Information	As defined by *Privacy Act 1988* (Cth), s 6(1), *sensitive information* is: a. 'Information or an opinion about an individual's: I. racial or ethnic origin; or II. political opinions; or III. membership of a political association; or IV. religious beliefs or affiliations; or V. philosophical beliefs; or VI. membership of a professional or trade association; or VII. membership of a trade union; or VIII. sexual orientation or practices; or IX. criminal record; that is also personal information; or b. health information about an individual; or c. genetic information about an individual that is not otherwise health information; or d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or e. biometric templates.'
Unsolicited Personal Information	Personal information received by AIE where no active steps have been taken to collect it.

6. Related Documents

The following internal documents are related to this policy:

a. Access/Correct Personal Information Form
b. AIE Policy Framework
c. Authority to Release Information Form
d. Domestic Student Complaints and Appeals Policy and Procedure
e. Education Agent Agreement
f. Information Technology Security Policy and Procedure
g. International Education Agent Register
h. International Student Complaints and Appeals Policy and Procedure
i. Learner Handbook
j. Student Document Retention and Credentials Policy and Procedure
k. Terms and Conditions of Enrolment (aie.edu.au).

The following legislation and standards are related to this policy:

l. Australian Privacy Principles
m. Australian Privacy Principles Guidelines (OAIC)
n. Archives Act 1983 (Cth)
o. Data Breach Preparation and Response (OAIC)
p. Do Not Call Register Act 2006 (Cth)
q. Education Services for Overseas Students Act 2000 (ESOS Act) (Cth)
r. Education Services for Overseas Students Regulations 2019 (Cth)
s. Freedom of Information Act 1982 (Cth)
t. National Code of Practice for Providers of Education and Training for Overseas Students 2018 (National Code 2018)
u. National Vocational Education and Training Regulator Act 2011 (Cth)
v. Privacy Act 1988 (Cth)
w. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
x. Spam Act 2003 (Cth)
y. Spam Regulations 2021 (Cth)
z. Standards for Registered Training Organisations (RTOs) 2015
aa. Student Identifiers Act 2014 (Cth)
bb. Student Identifiers Regulation 2014 (Cth).

7. Review

This policy will be reviewed annually by the National Compliance Officer.

8. Revision History

This policy has undergone the following revisions:

Version No.	Version Description	Contributor(s)	Approval Authority	Date Revised/ Approved
1.0	First version of document.	-	BOD	
1.1	Style update.	**Casey Gregory** (Manager, Planning and Implementation)	-	22 May 2017
2.0	Style update, content restructure, content edit, and content additions (definitions and related documents).	**Nick Markesinis** (Intranet Content Coordinator)	BOD	30 August 2021
3.0	Combined *Privacy Policy and Procedure* and *Personal Information Policy and Procedure* into one document, standardised for learners; updated procedures in line with APPs. Created *Access/Correct Personal Information Form* as an associated resource in fulfillment of APP12 and APP10.	**Nick Markesinis** (Intranet Content Coordinator) **Linda Burrows** (National Compliance Officer) **Charlotte Pichelmann** (National Compliance Administration Support)	BOD	29 August 2022