



PRIVACY POLICY AND PROCEDURE

Purpose

Australian Institute of Business (AIB) respects the privacy of individuals and is committed to managing and protecting personal and sensitive information fairly and lawfully. The purpose of this policy is to articulate the principles that lead to best practice management of personal data and information. To the extent that they apply to our activities, AIB will be consistent with the standards contained in the Commonwealth *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles, and will comply with the requirements of the European Union General Data Protection Regulation in respect of individuals located in the European Union (including the European Economic Area).

Scope

This policy applies to:

- (a) all personal information (including sensitive information) collected by AIB, including that of AIB staff, prospective and current students and other individuals associated with AIB, regardless of how it is processed or stored (electronically, in hardcopy, or by verbal means);
- (b) all areas of AIB and all AIB activities. All AIB employees (whether permanent, temporary, contractors, or consultants) and students must comply with the Privacy Policy and Procedure when collecting personal and sensitive information on AIB's behalf and when using or dealing with personal and sensitive information in AIB's possession.

Definitions

Unless otherwise defined in this document, all capitalised terms are defined in the [glossary](#).

Australian Privacy Principles means the set of 13 principles in the Privacy Act 1988 (Cth) governing the collection, quality, use, disclosure, management and security of personal information.

General Data Protection Regulation (GDPR) means the legal framework governing the collection and processing of personal information of individuals in the European Union (EU). The GDPR applies to entities outside the EU whenever they are processing the personal information of people in the EU.

Personal Information is defined in the Privacy Act 1988 (Cth) as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.' The types of Personal Information that AIB collects and holds will depend on the circumstance and relationship between the individual and AIB. Personal Information that is commonly collected by AIB includes:

- name
- address (residential, postal and email)
- phone number
- date of birth
- gender

- ethnic origin
- passport number
- banking and credit card details
- tax file number
- health information
- emergency contact details
- photographs or video recordings (including CCTV footage)
- criminal history
- academic record
- IT access logs
- metadata from use of online services and facilities
- records of donations and transactions

Sensitive Information is defined in the *Privacy Act 1988* (Cth) as:

- (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_

Policy

1. Principles

This policy supports the principle of responsible and transparent handling of personal data as required by the applicable privacy laws in processing personal data:

- 1.1. AIB respects the privacy of individuals and is committed to protecting and managing Personal and Sensitive Information fairly and lawfully.
- 1.2. Personal and Sensitive Information is collected for specified, explicit and legitimate purposes and is not further used in a manner that is incompatible with those purposes.
- 1.3. The information and data collected is limited to what is necessary in relation to the purposes.
- 1.4. The prevention of unauthorised or fraudulent access is achieved through robust technical, organisational and administrative measures.

Procedure

2. Collection of Personal Information

- 2.1. AIB will collect Personal Information by lawful and fair means and, where possible, directly from the individual. AIB collects Personal Information by various means including:
 - (a) from correspondence and submitted forms between an individual and AIB (including via phone and on-line portals)
 - (b) as part of any enrolment, appointment, registration or subscription process
 - (c) in the course of undertaking research
 - (d) direct contact in the course of providing services or administration of AIB activities;
 - (e) from third parties with which AIB collaborates
 - (f) monitoring and logging of metadata from individuals' use of IT and online services and facilities provided by AIB
 - (g) from CCTV cameras on AIB premises.
- 2.2. Personal Information collected by AIB may be held in hardcopy format, or electronic format stored on AIB's computing equipment or on third party servers.
- 2.3. Individuals will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection through the relevant Privacy Notice. In practical terms, this means that AIB will provide a Privacy Notice at each point where Personal Information is collected from an individual.
- 2.4. If AIB receives unsolicited Personal Information, and AIB has no lawful basis on which to retain the information AIB will destroy that information or ensure that it is de-identified.
- 2.5. AIB will not collect Sensitive Information unless:
 - (a) with the individual's consent or
 - (b) if required or authorised by Australian law or court/tribunal order or
 - (c) an exemption exists under the Privacy Act.
- 2.6. AIB's ability to provide products or services to an individual (such as enrolment in a course or the supply of appropriate information) will be affected if AIB is unable to collect the Personal Information AIB requires, or the information provided is incorrect or incomplete.

3. Use of Personal Information

- 3.1. All persons providing Personal Information to AIB under the provision of 2.1 and 2.3 of this Procedure are taken to consent to the use and disclosure of their Personal Information for the purposes stated in section 3.2.
- 3.2. The Personal Information that AIB collects is used by AIB or its contractors, representatives, advisers and agents for the primary purpose of providing an education service and for related purposes which include but are not limited to:
 - (a) marketing AIB products and services to past, current and potential students and graduates

- (b) Performing marketing analysis, such as customer or student profiling and segmentation
 - (c) communicating with past, current and potential students, staff, graduates, alumni, suppliers and enforcement bodies
 - (d) performing various administrative and academic functions including admissions, enrolments, teaching, proctoring online exams, marking and moderation of assessments, maintenance of business records including student and other records, addressing appeals and grievances, data storage, customer service, market profiling and statistical purposes
 - (e) corporate governance, auditing and record keeping
 - (f) compliance with AIB's legal and insurance obligations
 - (g) reporting obligations to government and regulatory bodies and other third parties including those listed in section 3. below
 - (h) internal planning, improvement and development
 - (i) recruiting and managing staff and contractors
 - (j) engaging and monitoring the performance of suppliers.
- 3.3. An individual can withdraw their consent to receiving direct marketing communications from AIB at any time by unsubscribing from the mailing list, by contacting AIB directly, or by using the opt out mechanism in AIB's direct marketing communications.
- 3.4. Sensitive Information will not be used for direct marketing or promotions unless an individual has given consent.

4. Disclosure of Personal Information

- 4.1. AIB will not disclose Personal Information, including Sensitive Information to parties not otherwise listed in 3.2 and 4.2 without an individual's consent, unless:
- (a) required or permitted by law.
 - (b) AIB has a reasonable belief that the use or disclosure is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body
 - (c) the disclosure of the Personal Information and/or Sensitive Information is necessary to deal with a serious and imminent threat to any individual's life or health.
 - (d) AIB has a reasonable belief that the use or disclosure is needed in order to take action on suspected unlawful activity or misconduct of a serious nature.
- 4.2. AIB may disclose Personal Information to the following types of third parties:
- (a) government departments and agencies
 - (i) The Tertiary Education Quality Standards Agency (TEQSA). A copy of TEQSA's privacy policy can be viewed at <http://teqsa.gov.au/privacy>.
 - (ii) The Department of Education, Skills and Employment, such as for the Unique Student Identifier for purposes relating to HESA and/or TEQSA; the Tuition Protection Services; obligations under the Higher Education Support Act and research undertaken for it by the Social Research Centre, which is an ANU business enterprise.
 - (iii) The Department of Home Affairs, such as in relation to regarding any visa requirements.
 - (iv) Other Government agencies and enforcement bodies, such as Commonwealth Government assistance with FEE-HELP, Centrelink or the

Australian Taxation Office, as well as their contractors, representatives and agents.

- (b) external service providers to the extent such Personal Information is required for the service provider to provide services to, or on behalf of, AIB, including but not limited to:
 - (i) externally hosted software and databases; surveys; third party peer review; citation checking; grading and plagiarism prevention service providers (including online providers) for academic, conduct or administrative purposes, such as for improving or checking of referencing of authorship or academic integrity.
 - (ii) Marketing or other service providers, including those that provide customer or student profiling and segmentation.
 - (iii) AIB's legal advisers or other professional advisers and consultants engaged by AIB.
- (c) third parties located outside of Australia
If AIB discloses Personal Information to an overseas recipient, AIB will:
 - (i) enter into a contract with the overseas recipient that binds the overseas recipient to privacy obligations that are consistent with the Australian Privacy Principles or GDPR or
 - (ii) ensure that the overseas recipient is subject to a law or binding scheme that has the effect of protecting the Personal Information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles and GDPR protect the information, and that individuals are able to access mechanisms to enforce the protection of the law or binding scheme or
 - (iii) obtain express consent of the individual to the disclosure of their Personal Information to the overseas entity.

4.3. AIB Subject webinars are automatically recorded. These webinars may involve the collection of personal information such as voice or image capture. Recordings are made available to the respective subject cohort to aid student learning and may be used for subject reviews, learning support and professional development purposes in subsequent cohorts.

- (a) AIB will make every effort to ensure that staff and students are aware that these webinars are recorded.

5. Integrity and Security of Personal Information

5.1. AIB takes all reasonable steps to ensure that:

- (a) the Personal Information it collects and discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure and
- (b) the Personal Information is protected, to the extent that is reasonable in the circumstances, from misuse, interference and loss, and from unauthorised access, modification or disclosure.

5.2. Where the Personal Information is no longer necessary for the purpose it was collected, that information will be either disposed of securely or de-identified if it is lawful and reasonable to do so.

- 5.3. While all reasonable measures have been made to secure information transmitted to the AIB website, individuals will be made aware that if they submit personal details, credit card numbers or other information, there is a possibility that this information may be observed by a third party while it is being transmitted.
- 5.4. Where the AIB website provides links to other websites, AIB is not responsible for the privacy practices or content of such websites.

6. Accountability and responsibilities

- 6.1. The Data Controller determines the purposes and means of processing personal information, deciding how and why personal information is processed. The AIB Chief Executive Officer is the Data Controller for the purposes of processing Personal Information.
- 6.2. The Privacy Officer manages requests for access, correction or erasure of Personal Information relating to students.
- 6.3. Human Resources manages requests for access, correction or erasure of Personal Information relating to employees.
- 6.4. The Data Protection Officer manages the processing of electronic Personal Information on behalf of the Data Controller. A Data Protection Officer is designated for each of the management, student and Learning systems.

7. Access to and Erasure or Correction of Personal Information

- 7.1. Individuals including AIB's students have the right to access their personal information, subject to limited exceptions in the Privacy Act and to have it corrected if the personal information is inaccurate, out of date, incomplete, irrelevant or misleading.
- 7.2. Individuals seeking access to, erasure or correction of, Personal Information:
 - (a) students must contact the Privacy Officer via Student Central
 - (b) employees must contact Human Resources
 - (c) other individuals may request access to Personal Information about themselves held by AIB by contacting the Company Secretary
 - (d) other individuals must contact the Privacy Officer via Student Central for access to Personal Information about individual students. Unless this information is required or permitted by law, the request for information must include a declaration of consent from the individual student to release that information
 - (e) the responsible officer will respond to requests promptly and generally within 20 working days of receipt.
- 7.3. An application fee for requesting access will not be charged, but if an individual's request for access is accepted, AIB will inform an individual of the fee (if any) that will be payable for providing access if an individual proceeds with their request.
- 7.4. Access to personal information may be denied by AIB in some circumstances, as specified in the Privacy Act.

- 7.5. If AIB refuses to give access to, or to erase or correct the personal information as requested by an individual, AIB will give an individual a written notice that sets out the reasons for the refusal (except to the extent that it would be unreasonable to do so), the mechanisms available to complain about the refusal and any other matter prescribed by the regulations.

8. Reporting Data and Privacy Incidents

- 8.1. A data or privacy incident means an actual or suspected data breach as defined under applicable privacy laws, including:
- (a) the use or disclosure of personal data for a purpose that is not authorised by the individual or by law or
 - (b) the loss, accidental or unlawful destruction, misuse, unauthorised access, alteration or disclosure of personal data.
- 8.2. Data or privacy breaches must be reported immediately to the Data Controller.
- 8.3. The Data Controller may form a Data Breach Review Group with responsibility for:
- (a) containing, assessing and responding to significant data breaches in a timely and consistent manner and
 - (b) determine if there is a need to notify affected individuals, the Office of the Australian Information Commissioner or others, having regard to any mandatory data breach reporting requirements under legislation, contract or binding code.

9. Complaints

- 9.1. Individuals who believe that a breach of their privacy has occurred or otherwise have a complaint about the use of their Personal Information should make a complaint in writing to:
- Privacy Officer
Australian Institute of Business
Level 16, 1 King William St,
Adelaide, South Australia 5000
Or by email: quality@aib.edu.au
- 9.2. Within 10 working days after details of the complaint are received by AIB, AIB will provide a written notice that acknowledges receipt of the complaint and will set out how AIB will deal with the complaint.
- 9.3. The complaint will be reviewed and a substantive response made within a reasonable time (usually 20 working days from the date the complaint was received).
- 9.4. Any individual who is dissatisfied with the outcome of the complaint may refer the matter to the Office of the Australian Information Commissioner at:
- Website: <https://www.oaic.gov.au/>
Phone: 1300 363 992.

10. Changes to AIB's Privacy Policy

10.1. AIB may amend, modify or replace this Privacy Policy at any time. Individuals that provide personal information or entities that provide third parties' personal information to AIB should review AIB's Privacy Policy each time they visit AIB's website or provide AIB with personal information.

Related Policies and Procedures:

Privacy Procedure

Whilst many Policies and Procedures relate to the Privacy Policy and Procedure, the following Policies and Procedures assist AIB to comply with its privacy obligations:

Academic Facilities Policy and Procedure

Acceptable Use of Information Technology (IT) Facilities Policy and Guidelines for Students

Payment Card Information Handling Policy and Procedure

Records Management Policy and Procedure

Responsible Research Conduct Policy and Procedure

Legislative references:

Privacy Act 1988 (Cth)

South Australian Cabinet Administrative Instruction 1/89 (Information Principles Instruction)

Higher Education Support Act 2003 (Cth)

Privacy (Tax File Number) Rule 2015 (Cth)

Telecommunications (Interception and Access) Act 1979

Freedom of Information Act 1991 (SA)

Regulation EU 92016/679)-General Data Protection Regulation (GDPR)

Do Not Call Register Act 2006

Responsibility:

Chief Executive Officer

| | |
|-----------------------------|---|
| Current Status: | Version 1 |
| Approved By: | Board of Directors |
| Date of Approval: | 9 February 2023 |
| Effective From: | 20 February 2023 |
| Previous Versions: | 18 November 2021 (<i>Privacy Policy V7.0 and Privacy Procedure V1.1</i>) 31 March 2021 3 December 2020 5 March 2020 2 October 2019 29 May 2019 27 November 2018 23 June 2016 4 February 2015 <i>Student Personal Information Policy V3 and Privacy and Personal Information Procedures V3</i> 1 July 2011 27 October 2008 |
| Date of Next Review: | 18 November 2024 |