PRIVACY PROCEDURE

Policy Code	OPS13
Policy Lead	Chief Executive Officer / Principal
Approving Authority	Board of Directors
Approval date	27 June 2024
Commencement date	01 July 2024
Next Review Date	April 2027
Version	2024.2
Relevant legislation or external requirements	National Code of Practice for Providers of Education and Training to Overseas Students 2018 (N: 3.3.6) Higher Education Standards Framework (Threshold Standards) 2021 (HESFs:7.3.1 a-d) Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act) Education Services for Overseas Students Act 2000 (Cth) (ESOS Act) Education Services for Overseas Students Regulations 2019 (Cth) (ESOS Regulations) Health Records and Information Privacy Act 2002 (NSW) (HRIP Act). Health Privacy Principals (HPPs) NSW (https://www.ipc.nsw.gov.au/health-privacy-principles-hpps-explained-members-public) Privacy Act 1988 (Cth) Privacy Act 1988 Schedule 1 Australian Privacy Principles Privacy Amendment (Enhancing Privacy Protection) Act 2012 Privacy and Data Protection Act 2014
Related ASA Documents	Artificial Intelligence Policy and Procedure Critical Incident Management Plan Critical Incident Policy Cyber Security Framework Cyber Security Procedure Discrimination, Bullying and Harassment Policy and Procedure Fraud Policy and Procedure Information Technology Policy and Procedure Records and Information Management Policy and Procedure Sexual Assault and Sexual Harassment Policy and Procedure Staff Code of Conduct Staff Induction Policy Staff Induction Procedure Student Grievance Policy Student Grievance Procedure Work Health and Safety Policy Work Health and Safety Procedure

1. Purpose

The ASA Institute of Higher Education (**ASA**) commits to its obligations under the *Privacy Act 1988* (revised) and the *Australian Privacy Principles* (**APPs**). This document describes how ASA collects, uses, discloses and handles certain information in compliance with the 13 APPs as required by the applicable Privacy Act.

2. Scope

This Procedure applies to all ASA applicants, students, staff, directors, officers, external appointees on any ASA board or committee, volunteers, visitors, and contractors.

3. Procedures

ASA staff, students and agents operating on ASA's behalf, are expected to comply with ASA's *Privacy Policy* and relevant privacy legislation including the *Australian Privacy Principles* (APPs) and the *Health Privacy Principles* (HPPs). This procedure is intended to assist with compliance and is not a substitute for any State or Government privacy legislation.

ASA takes reasonable steps to ensure that the information they hold is accurate, complete, and up to date.

3.1 Collecting information

When collecting information about an individual, the following guidelines are recommended:

a. Only collect information if it is needed (i.e. only collect information if it is necessary for one or more of ASA's functions and activities);

b. Wherever possible, collect the information directly from the individual concerned;

c. Ensure that the information is collected lawfully, securely and fairly;

d. Ensure the collection is not unreasonably intrusive; and

e. Inform individuals in writing that their information is being collected, why it is being collected and how it is to be used.

3.2 Collecting sensitive information

Sensitive information is defined in the *Privacy and Data Protection Act 2014* and includes religious, political, or sexual preference information. It must only be collected if it is essential for ASA's operations. In addition, sensitive information should not be collected unless:

a. the individual has provided their informed consent in writing;

b. the collection is required by law;

c. it is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual; or

d. it is necessary for the establishment, exercise or defence of a legal or equitable claim.

However, ASA may collect sensitive information about an individual if:

a. the collection

   i. is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

   ii. the collection is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government-funded targeted welfare or educational services; and

b. there is no reasonably practicable alternative to collecting the information for that purpose; and

c. it is impractical for ASA to seek the individual's consent to the collection.

3.3 Collecting health information

Health information is very broadly defined in the Health Records and Information Privacy Act 2002 (NSW) and includes information or an opinion about the physical, mental or psychological health of an individual or a disability or a health service provided to an individual.

The collection of health information is subject to very stringent legislative requirements and it must only be collected if it is essential for ASA's operations. Health information should not be collected unless the individual has provided their consent or in accordance with the limited exceptions set out in the HPP1 as below:

Purposes of collection of health information

(1) An organisation must not collect health information unless—

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

3.4 Anonymity

Individuals generally have the option of not identifying themselves when dealing with ASA. Such a request should be accommodated wherever lawful and practicable. However, the person should be advised that ASA may not be able to provide services to them because the nature of ASA's work means that it is generally not possible to provide services to, or interact with, students or staff in an anonymous way.

3.5 Disclosing information

ASA will not disclose personal or sensitive information to third parties outside ASA unless it:

- has the written consent of the individual concerned;
- has a duty of care to disclose this information to the Police and a parent/guardian of a student or visitor under the age of 18;
- is required to do so by legislation, court order or other legally enforceable instrument received inappropriate written form; and
- reasonably believes disclosure to be necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

ASA will ensure that business partners (local or overseas), such as agents, contractors and cloud computing providers are made aware of these requirements with respect to information shared with them in the course of ASA business.

ASA will deal promptly with any unauthorised disclosures of personal information.

3.6 Access to and correction of personal information

Students, or appropriately authorised third parties, may seek access and request corrections to the personal and sensitive information collected about them by contacting the Director Student Experience. Access may be denied if such access would have an unreasonable impact on the privacy of others, or where such access may result in a breach of ASA's duty of care to the student concerned. Authorised corrections will be made within ten (10) working days and without charge.

Staff and Board/Committee members may seek access and request corrections to the personal and sensitive information collected about them by contacting the Chief Executive Officer. Access

may be denied if such access would have an unreasonable impact on the privacy of others, or where such access may result in a breach of ASA's duty of care to the staff member concerned. Authorised corrections will be made within ten (10) working days and without charge.

Other individuals external to ASA may contact the Director Student Experience in writing and will be advised within ten (10) working days of receiving the written request of how they may access or obtain a copy of their personal information.

3.7 Securing, storing and retaining data

ASA stores information using electronic and hardcopy record systems. All staff and each operational area must take reasonable steps to ensure that:

a. information is protected from misuse, loss, unauthorised access or modification, or improper disclosure;

b. practices, procedures and systems (including electronic and physical) are in place to ensure that the information is stored (and if necessary moved) safely and securely;

c. the information has not been changed or been tampered with;

d. all records containing personal, sensitive and health information are kept in a secure location and cannot be accessed by unauthorised persons;

e. Authentication processes (for identification) are adhered to, in that a person accessing or providing information are who they claim to be; and

f. requirements around retention of information are complied with, according to the *Records and Information Management Policy and Procedure*.

4. Disposing of and destroying information

It is a requirement that records, and information must be maintained securely and not damaged, altered, or destroyed without proper authorisation. All records and information must be available for authorised access as and when required. Physical records and information will be securely shredded. Digital records and information will be deleted from systems and, if relevant, deleted from secondary repositories.

Records and information may be destroyed or safely disposed of only if:

- the appropriate retention period has expired;
- proper authorisation to dispose of a record or records and information has been obtained; and
- the record or records and information are not required to be kept for a longer period by any relevant legislation.

Records and information which must be held indefinitely, and non-current or historical records and information, will be archived. See Appendix A in the *Records and Information Management Policy and Procedure* for retention periods.

5. Roles and Responsibilities

5.1 Chief Executive Officer

The Chief Executive Officer is responsible for overseeing ASA compliance with the requirements of Australian privacy legislation, and for ensuring that all Board and Committee Members and Senior Management team members are aware of the *Australian Privacy Principles* and apply these to their areas of operation. This includes contracts with external business partners. As part of Induction and onboarding processes, training on the *Australian Privacy Principles* will be

provided to all Board and Committee Members and Senior Management team members. The details are listed in *Governance Member Induction Manual*.

The Chief Executive Officer has the responsibility to manage responses from staff and Board/Committee members who seek access and request corrections collected by ASA about their personal and/or sensitive information.

5.2 Director Student Experience

The Director Student Experience has the delegated responsibility for the implementation of the Policy across ASA and for ensuring operational compliance. This includes the provision of ongoing training for staff, provision of appropriate information for students and the public, and recording and reporting (where required) of complaints and any other Policy breaches.

The Director Student Experience as Registrar is responsible for the safe storage and handling of student personal details, student academic enrolment details, student correspondence, academic results, student personal files, student administration archives.

5.3 Academic Dean

The Academic Dean, or delegate, has the responsibility of the safe storage and handling of student assessments and all course details. Safe storage and handling of confidential student counselling records will be delegated to the Wellbeing Officer.

5.4 Director Quality and Compliance

The Director Quality and Compliance is responsible for the safe storage and handling of proof of course accreditation, registration, certification and accuracy of policy and procedures in relation to legislation of the Privacy Act.

5.5 Finance/Accountant

The Accountant will manage the safe storage and handling of student financial details including agent and student related correspondence. The Accountant has the responsibility of the safe storage and handling of payroll records and financial day to day operations. The Finance Manager is responsible for the back up of all financial records management.

5.6 Staff/Students

All staff and students are responsible for understanding and complying with the provisions of this Procedure and associated policy.

6. Version Control

This Procedure has been reviewed and approved by the ASA Board of Directors as at June 2024 and is reviewed every three years.

The Procedure is published and available on the ASA website https://www.asahe.edu.au/policies-and-forms/.

Change and Version Control				
Version	**Authored by**	**Brief Description of the changes**	**Date Approved:**	**Effective Date:**
2024.2	Academic Dean	Minor update adding reference to the Artificial Intelligence Policy and Procedure	27/06/2024	01/07/2024
2024.1	Chief Operating Officer	Updated policy to include HESF references, changes in regulatory compliances. Benchmarked against 10 other Higher Education Providers.	26/04/2024	08/05/2024
Previous version archived. New Policy code and numbering system implemented.				
2.1		Board of Directors approval	04/11/2020	