



Institute of International Studies

RTO CODE 45883

POLICY & PROCEDURES · PRIVACY AND DATA PROTECTION

Privacy

Policy and Associated Procedures

POLICY AREA	Privacy, Data Protection, Information Security, and Confidentiality Management
STANDARDS REFERENCE	Outcome Standards 2.1 and 4.1; Privacy Act 1988 (Cth) and Australian Privacy Principles
RESPONSIBILITY	CEO, RTO Manager, Compliance Manager, Administrative Staff, Trainers and Assessors
CLASSIFICATION	Privacy, Data Protection, and Records Management Policy (publicly available)

01 Purpose

The purpose of this Privacy Policy and Associated Procedures is to outline the Institute of International Studies (IOIS) approach to the collection, use, storage, disclosure, and protection of personal information. IOIS is committed to safeguarding the privacy of students, staff, contractors, and other stakeholders and to ensuring that personal information is handled **lawfully, ethically, and securely**.

This policy establishes clear requirements for managing personal information throughout its lifecycle, including collection, access, use, disclosure, retention, and disposal. It ensures that personal information is collected only for legitimate and necessary purposes related to the delivery of education and training services and organisational operations.

The policy supports transparency by informing individuals about how their personal information is managed and their rights in relation to that information, including access and correction rights. It also sets out IOIS's responsibilities in responding to privacy complaints, data breaches, and unauthorised access or disclosure.

This policy ensures compliance with the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**, the Student Identifiers Act 2014 (Cth), national VET data reporting requirements, and relevant requirements under the Standards for RTOs 2025. This policy is published on the IOIS website and is available free of charge on request.

02 Scope

This Privacy Policy and Associated Procedures apply to all personal information collected, held, used, or disclosed by the Institute of International Studies (IOIS) in the course of its operations.

- The policy applies to all personal information relating to students, prospective students, trainers and assessors, staff, contractors, education agents, and any other third parties who engage with IOIS. This includes information collected during enquiry, enrolment, training and assessment, student support, certification, employment, and business operations.
- This policy applies across all IOIS delivery modes, and to any IOIS-managed or IOIS-approved systems and platforms used to collect, store, access, manage, or disclose personal information.
- The policy also applies to all IOIS staff and representatives who handle, access, manage, or process personal data on behalf of IOIS. All such individuals are required to comply with this policy and associated procedures.

03 Policy Statements

3.1 Collection of Personal Information

- IOIS collects personal information in a lawful, fair, and transparent manner and only for purposes that are directly related to the delivery of education and training services, student support, and organisational operations. Wherever practicable, personal information is collected directly from the individual to whom the information relates.
- Personal information is collected through a range of approved methods, including enrolment and application forms, Course Entry Interviews, assessments, surveys, learning management systems, email correspondence, and other formal communications between IOIS and the individual.
- Where it is lawful and practicable, individuals may deal with IOIS anonymously or using a pseudonym, for example when making a general enquiry. This is not possible for enrolment, assessment or certification.

The types of personal information collected by IOIS may include, but are not limited to:

CONTACT DETAILS

Full name, residential or postal address, telephone number, and email address.

DEMOGRAPHIC INFORMATION

Age, gender, nationality, and other information required for national VET data reporting or support purposes.

UNIQUE STUDENT IDENTIFIER (USI)

Collected and verified as required by the Student Identifiers Act 2014 before AQF certification can be issued.

ACADEMIC HISTORY

Qualifications, transcripts, records of results, and evidence submitted for Credit Transfer or Recognition of Prior Learning.

IDENTIFICATION DOCUMENTS

Where required to confirm identity for enrolment, assessment, certification, or verification purposes.

SUPPORT NEEDS

Disclosed disability, language, literacy, numeracy, or digital literacy requirements, provided voluntarily to enable appropriate support or reasonable adjustments.

EMERGENCY CONTACTS

Collected to ensure student and staff safety and wellbeing.

FINANCIAL INFORMATION

Payment, invoice and refund details needed to administer fees.

IOIS limits the collection of personal information to that which is reasonably necessary for enrolment, training and assessment delivery, learner support, compliance with regulatory requirements, and the issuance and verification of certification. Personal information that is not required for these purposes is not collected.

3.2 Use of Personal Information

IOIS uses personal information only for purposes that are directly related to its education, training, and organisational functions and that would be reasonably expected by the individual at the time of collection.

Personal information collected by IOIS may be used for the following purposes:

- Processing and managing enrolment applications, including assessing eligibility, confirming entry requirements, and establishing student records.
- Delivering and administering training and assessment, including learning management, assessment marking, feedback, moderation, and validation activities.
- Issuing and verifying certification, including qualifications, statements of attainment, and records of results.
- Providing academic, wellbeing, and support services to students, including identifying support needs, implementing reasonable adjustments, and coordinating referrals where required.
- Communicating with students and other stakeholders, including providing course-related updates, notices, outcomes, policy information, and responses to enquiries or complaints.
- Meeting compliance and reporting obligations, including obligations under the Standards for RTOs 2025, national VET data reporting (AVETMISS), the Australian Qualifications Framework (AQF), and other applicable legislative and regulatory requirements.

Personal information is not used for purposes unrelated to IOIS operations unless required or authorised by law or with the individual's consent. IOIS does not use personal information for direct marketing without the individual's consent, and every marketing communication includes a simple way to opt out.

3.3 Storage and Security

- IOIS takes reasonable and appropriate steps to ensure that personal information is stored securely and protected against misuse, interference, loss, unauthorised access, modification, or disclosure.
- Personal information is stored primarily in IOIS's Student Management System (SMS), Learning Management System (LMS), and other approved internal databases. These systems are configured to support secure data management and are maintained in accordance with organisational and regulatory requirements.
- Access to personal information is restricted to authorised staff only, based on role responsibilities and the principle of least privilege. Access rights are reviewed periodically.
- IOIS implements technical and administrative security measures, which may include password protection, multi-factor authentication, restricted network access, secure servers, and encryption where applicable. Systems are monitored to reduce the risk of unauthorised access or data breaches.
- Where personal information is held in hard copy form, records are stored in locked filing cabinets or secure storage areas with controlled access.

3.4 Disclosure of Personal Information

IOIS respects the confidentiality of personal information and does not disclose personal information to third parties without the individual's consent, unless such disclosure is required or authorised by law. Personal information may be disclosed in limited circumstances where it is necessary to meet regulatory, contractual, or operational obligations, including to:

NCVER and government agencies	The National Centre for Vocational Education Research (NCVER), the Commonwealth Department responsible for VET, and State or Territory training authorities, as required under national VET data reporting requirements. Students are informed of this through the national VET Privacy Notice included in the enrolment form.
Student Identifiers Registrar	To verify or create a student's USI and to enable access to their authenticated VET transcript.
ASQA and other regulators	Where disclosure is required under legislation, regulatory standards or an audit.
External auditors and validators	For compliance monitoring, validation, or audit activities.
Service providers	Providers engaged by IOIS, such as information technology support or system hosting, where access is necessary to perform those services, under confidentiality and data protection agreements.

Overseas disclosure: where personal information is stored by, or disclosed to, a service provider located outside Australia (for example, a cloud-hosted system), IOIS takes reasonable steps to ensure the provider handles the information consistently with the Australian Privacy Principles, and identifies the countries involved in its privacy notice where practicable.

IOIS does not sell, trade, or otherwise commercially exploit personal information under any circumstances. Any disclosure of personal information is limited to what is reasonably necessary for the purpose.

3.5 Access and Correction

- IOIS recognises the right of individuals to access and correct their personal information held by the organisation and is committed to maintaining accurate, complete, and up-to-date records.
- Students, staff, and other individuals may request access to their personal information held by IOIS at any time. Requests must be made in writing to the Administration Office and should clearly identify the information being sought.
- IOIS will respond to access requests and provide the requested information within **ten (10) working days**, unless there are lawful grounds for refusing access. Where access is refused or limited, IOIS will provide written reasons and information about how to complain.

- Individuals may also request correction of personal information where it is believed to be inaccurate, incomplete, out of date, or misleading. Where IOIS does not agree that a correction is required, the individual will be informed of the reasons and may ask for a statement to be associated with the record.

3.6 Retention and Disposal

RETENTION SCHEDULE AT A GLANCE

30 YEARS AQF certification records	5 YEARS Enrolment, administrative and financial records	2 YEARS Student assessment evidence	As needed Other personal information
--	---	---	--

- IOIS retains personal information only for the period necessary to meet educational, operational, regulatory, and legal obligations, applying clear retention timeframes in accordance with the Standards for RTOs 2025 and relevant legislation.
- Records that relate to AQF certification outcomes, including qualifications, Statements of Attainment, and records of results, are securely retained for **thirty (30) years**. This enables verification of credentials, reissue of certification, and compliance with audit and regulatory requirements.
- Enrolment and administrative student records, including enrolment forms, student agreements, identification and eligibility records, admission records, enrolment correspondence, withdrawal records, and cancellation records, are securely retained for a minimum of **five (5) years** following the student's completion, withdrawal, cancellation, or last enrolment activity, unless a longer period is required. Financial records are retained for at least five years, consistent with taxation requirements.
- Student assessment evidence, including completed assessment submissions, RPL evidence, assessor-marked work, observation records, third-party reports, and evidence used to support assessment judgements, is securely retained for a minimum of **two (2) years** after the student has completed the relevant training product, unless a longer retention period is required.
- Other personal information, including student support documentation, general correspondence, internal records, and administrative documentation, is retained only for as long as reasonably required for the purpose for which it was collected, or as otherwise required by law, regulation, contractual obligation, audit, complaint, appeal, investigation, or IOIS's approved records retention schedule.
- Once retention periods have expired and the information is no longer required, IOIS ensures that records are disposed of using secure and irreversible methods. Hard copy records are destroyed by shredding, and electronic records are permanently deleted or securely de-identified.

3.7 Data Breaches

IOIS responds promptly to any actual or suspected data breach, including unauthorised access to, disclosure of, or loss of personal information, in accordance with the **Notifiable Data Breaches (NDB) scheme** under the Privacy Act 1988.

STEP 1 Contain Take immediate steps to contain the breach and limit further access or disclosure.	STEP 2 Assess Assess whether the breach is likely to result in serious harm, completing the assessment within 30 days.	STEP 3 Notify If it is an eligible data breach, notify the OAIC and affected individuals as soon as practicable.	STEP 4 Review Record the breach, review its causes and implement improvements.
---	--	--	--

Serious breaches are also managed under the IOIS Critical Incident Policy and Associated Procedures.

3.8 Complaints

- IOIS is committed to managing privacy concerns promptly, fairly, and transparently.
- Individuals who believe that their privacy has been breached may lodge a complaint in accordance with the IOIS Complaints Policy and Associated Procedures. Complaints are investigated impartially, and appropriate corrective actions are implemented where a breach is identified. The complainant is informed in writing of the outcome and any actions taken.
- Where a privacy complaint cannot be resolved internally to the satisfaction of the individual, they may escalate the matter to the **Office of the Australian Information Commissioner (OAIC)** at www.oaic.gov.au. IOIS cooperates fully with any external investigation and implements any recommendations or determinations arising from such reviews.

04 Procedures

4.1 Collecting Information

- IOIS collects only information that is reasonably necessary for enrolment, delivery of training and assessment, student support, certification, compliance, and organisational operations, at the point of enrolment or through ongoing contact with students, staff, or other stakeholders.
- At the time of collection, IOIS clearly explains the purpose for which the personal information is being collected, how it will be used, and any circumstances in which it may be disclosed. For students, this includes the **national VET Privacy Notice and Student Declaration** in the enrolment form, which explains disclosure to NCVER and government agencies.
- Where sensitive information is collected, such as information relating to disability, health, support needs, or other personal circumstances, IOIS obtains the individual's informed consent prior to collection. Sensitive information is collected only where necessary and is handled with a higher level of confidentiality and security.

4.2 Storing Information

- Personal information collected by IOIS is entered promptly into secure electronic systems, including the SMS, LMS, or other approved databases, supporting accuracy, data integrity, and effective record management.
- Where personal information is held in physical form, records are stored in locked filing cabinets or secure storage areas accessible only to authorised personnel.
- Access to all personal information is restricted to authorised personnel only, based on role responsibilities and operational need, and permissions are reviewed periodically.

4.3 Disclosing Information

- Prior to disclosing any personal information to a third party, IOIS confirms the legal authority or consent permitting the disclosure, such as written consent from the individual, a legislative or regulatory requirement, or a necessary IOIS function.
- Details of disclosures of personal information outside routine regulatory reporting are formally recorded, including what information was disclosed, to whom, the purpose, and the date.
- Where IOIS engages third-party service providers that require access to personal information, contracts include confidentiality and data protection clauses that require them to handle personal information securely, restrict use to authorised purposes, and comply with applicable privacy legislation.

4.4 Access and Correction

- All requests for access to personal information or for correction of records must be received in writing and directed to the Administration Office.
- Before releasing any personal information, IOIS verifies the identity of the individual making the request. Where a request is made by a third party, appropriate written authority must be provided.
- IOIS provides access to the requested personal information within ten (10) working days, unless there are lawful grounds for refusal, in which case written reasons are given.
- Where corrections are requested and accepted, IOIS updates record promptly across relevant systems and confirms the correction to the individual.

4.5 Responding to a Data Breach

- Any staff member who becomes aware of an actual or suspected data breach must report it immediately to the RTO Manager and the IT Administrator.
- The RTO Manager coordinates containment and the assessment of whether the breach is likely to result in serious harm, completing the assessment within 30 days.
- If the breach is an eligible data breach, the CEO ensures the OAIC and affected individuals are notified as soon as practicable, with information about the breach and recommended steps.
- All breaches, assessments and actions are recorded, and improvements are entered in the Continuous Improvement Register.

4.6 Complaints

- Privacy-related complaints are managed in a fair, timely, and transparent manner in accordance with the IOIS Complaints Policy and Associated Procedures.
- All privacy complaints are investigated impartially, with appropriate corrective actions implemented where a breach is identified, and the complainant is informed in writing of the outcome.
- Where a privacy complaint cannot be resolved internally, IOIS provides the complainant with the OAIC's contact details and information on how to escalate the matter.

05 Responsibilities

ROLE	RESPONSIBILITIES
Chief Executive Officer (CEO)	Ensures IOIS complies with the Privacy Act 1988 (Cth) and the Australian Privacy Principles, with appropriate policies, systems, and resources in place, and ensures eligible data breaches are notified to the OAIC and affected individuals.
RTO Manager	Oversees data management practices, ensuring personal information is collected, used, and disclosed in accordance with this policy, approving external disclosures where required, coordinating data breach responses, and monitoring compliance with privacy obligations.
Administration and Student Support Officer	Manages personal information day to day, including collecting, storing, updating, accessing, and securely disposing of personal data in accordance with approved procedures and maintaining accurate records.
Trainers and Assessors	Protect student confidentiality during training and assessment, handling assessment evidence and student information securely and ensuring personal information is not disclosed inappropriately during delivery, assessment, or feedback.

06 Related Documents and Legislation

IOIS DOCUMENTS

- Student Handbook
- Staff Handbook
- Enrolment Form (including the VET Privacy Notice)
- Student Support Policy
- Complaints Policy and Associated Procedures
- Critical Incident Policy and Associated Procedures
- Records Management Procedure

LEGISLATION AND REQUIREMENTS

- Privacy Act 1988 (Cth) and Australian Privacy Principles
- Notifiable Data Breaches scheme (Part IIIC, Privacy Act)
- Student Identifiers Act 2014 (Cth)
- National VET Data Policy and AVETMISS requirements
- Standards for RTOs 2025



Document Version Control

DOCUMENT TITLE	IOIS Privacy Policy and Associated Procedures
REVIEWED BY	Compliance Manager
APPROVED BY	Chief Executive Officer
NEXT REVIEW DUE	October 2027

VERSION	CHANGELOG	DATE
1.0	New document	July 2025
1.1	Minor revision to update enrolment record retention period from two (2) years to five (5) years to align with organisational requirements and regulatory expectations. No other changes to privacy principles, data handling, or compliance framework.	June 2026
1.2	Revised: NCVER, government agency and USI Registrar disclosures and the VET Privacy Notice added; Notifiable Data Breaches procedure added; overseas disclosure, anonymity and direct marketing (APPs 2, 7, 8) added; policy marked publicly available; outdated Compliance Standards references removed; Academic Manager replaced by RTO Manager; complaints routed to the Complaints Policy	October 2026