Institute of International Studies (IOIS)
ABN: 86636830263 RTO: 45883
Address: Suite 703, Level 7, 79 George Street
Parramatta, NSW-2150
https: www.iois.edu.au

# Privacy Policy and Associated Procedures

| | |
|---|---|
| Policy Area: | Privacy, Data Protection, Information Security, and Confidentiality Management |
| Standards Reference: | Outcome Standard 2.1, 4.1, Compliance Standard 19 & Compliance Standard 20 |
| Responsibility: | CEO, RTO Manager, Compliance Officer, Administrative Staff, Trainers and Assessors, Student Support Officer |
| Classification: | Internal Privacy, Data Protection, and Records Management Policy |

## 1. 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)**, as well as relevant requirements under the **Standards for RTOs 2025**, particularly those relating to learner protection, recordkeeping, and confidentiality. It applies to both domestic and offshore operations and supports best practice in information governance and data protection.

## 2. 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 locations and modes, including offshore operations, online and blended delivery, and any IOIS-managed or IOIS-approved systems and platforms used to collect or store 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 to ensure that personal information is managed in a secure, confidential, and lawful manner at all times.

## 3. 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.
- The types of personal information collected by IOIS may include, but are not limited to:
    - **Contact details**, such as full name, residential or postal address, telephone number, and email address.
    - **Demographic information**, including age, gender, nationality, or other information required for reporting or support purposes.
    - **Academic history and prior learning evidence**, including 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.
    - **Information relating to support needs**, such as disclosed disability, language, literacy, numeracy, or digital literacy requirements, provided voluntarily to enable appropriate support or reasonable adjustments.
    - **Emergency contact details**, collected to ensure student and staff safety and wellbeing.
- 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, 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.

### 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. Staff are provided access only to the information necessary to perform their duties, and access rights are reviewed periodically.
- IOIS implements a range of **technical and administrative security measures** to protect personal information. These measures may include password protection, secure user 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. Hard copy records are accessible only to authorised personnel and are handled in a manner that maintains confidentiality and privacy at all times.

### 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. This may include disclosure to:

- **External auditors or reviewers** for the purposes of compliance monitoring, validation, or audit activities.
- **Government regulators or authorities**, such as ASQA or other relevant bodies, where disclosure is required under legislation or regulatory standards.
- **External service providers** engaged by IOIS to deliver specific services, such as information technology support or system hosting, where access to personal information is necessary to perform those services. In such cases, IOIS ensures that appropriate confidentiality and data protection agreements are in place.

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 and is managed in accordance with this policy and applicable privacy legislation.

### 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 to enable timely processing.
- 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 for the decision in accordance with privacy legislation.
- Individuals may also **request correction** of personal information where it is believed to be inaccurate, incomplete, out of date, or misleading. Upon receiving a correction request, IOIS will take reasonable steps to update the information promptly and confirm the correction in writing. Where IOIS does not agree that a correction is required, the individual will be informed of the reasons and advised of available options to have a statement associated with the record.

### 3.6 Retention and Disposal

- 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.
- All other personal information, including enrolment records, assessment materials, correspondence, and student support documentation, is retained for a **minimum of two (2) years** following a student's completion or withdrawal, unless a longer period is required by law or justified by operational needs.
- 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 to prevent reconstruction, unauthorised access, or misuse.

### 3.7 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 and Appeals Policy**. 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)**. IOIS cooperates fully with any external investigation and implements any recommendations or determinations arising from such reviews.

## 4. Procedures

### 4.1 Collecting Information

- IOIS applies a controlled and transparent approach to the collection of personal information to ensure compliance with privacy legislation and to protect individual rights.
- IOIS collects only information that is reasonably necessary for enrolment, delivery of training and assessment, student support, certification, compliance, and organisational operations. Information is collected at the point of enrolment or through ongoing contact with students, staff, or other stakeholders, and is limited to what is required to perform IOIS functions effectively.
- 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. This information is communicated through enrolment forms, interviews, policy documents, and direct communication, ensuring that individuals are informed and aware.
- 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 to provide appropriate support or meet legal obligations and is handled with a higher level of confidentiality and security in accordance with this policy.

### 4.2 Storing Information

- IOIS ensures that personal information is stored securely to protect confidentiality and prevent unauthorised access, loss, or misuse.
- Personal information collected by IOIS is **entered promptly into secure electronic systems**, including the Student Management System (SMS), Learning Management System (LMS), or other approved databases. Timely data entry supports accuracy, data integrity, and effective record management.

- Where personal information is held in **physical or hard copy form**, records are stored in locked filing cabinets or secure storage areas with controlled access. These areas are accessible only to authorised personnel and are managed to prevent unauthorised removal or viewing of records.
- Access to all personal information is **restricted to authorised personnel only**, based on role responsibilities and operational need. IOIS applies access controls and reviews permissions periodically to ensure that only those with legitimate reasons can access personal data, in accordance with this policy and applicable privacy requirements.

### 4.3 Disclosing Information

- IOIS applies strict controls to the disclosure of personal information to ensure that privacy obligations are met and that information is released only in appropriate and authorised circumstances.
- Prior to disclosing any personal information to a third party, IOIS confirms the legal authority or consent permitting the disclosure. This may include verifying written consent from the individual, confirming a legislative or regulatory requirement, or establishing that the disclosure is necessary to perform IOIS functions in accordance with this policy.
- Details of all disclosures of personal information are formally recorded, including what information was disclosed, to whom it was disclosed, the purpose of the disclosure, and the date on which the disclosure occurred. These records support accountability, transparency, and audit requirements.
- Where IOIS engages third-party service providers that require access to personal information, IOIS ensures that appropriate contractual arrangements are in place. Contracts and agreements include confidentiality and data protection clauses that require third parties to handle personal information securely, restrict use to authorised purposes only, and comply with applicable privacy legislation and IOIS requirements.

### 4.4 Access and Correction

- IOIS follows a clear and secure process to manage requests for access to, or correction of, personal information in accordance with privacy legislation and this policy.
- All requests for access to personal information or for correction of records must be received in writing and directed to the Administration Office. Requests must clearly identify the information being sought or the correction requested to enable efficient processing.
- Before releasing any personal information, IOIS verifies the identity of the individual making the request to ensure that information is disclosed only to the authorised person. 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. Where access is refused or limited, IOIS advises the individual in writing of the reasons in accordance with privacy requirements.
- Where corrections are requested and accepted, IOIS updates records promptly to ensure that personal information is accurate, complete, and current. Confirmation of the correction is provided to the individual, and updated information is reflected across relevant systems where applicable.

### 4.5 Complaints

- IOIS manages privacy-related complaints in a fair, timely, and transparent manner in accordance with the **IOIS Complaints and Appeals Policy**. Individuals who believe their personal information has been mishandled, disclosed without authority, or otherwise treated in breach of this policy may lodge a formal complaint using the established complaints process.
- All privacy complaints are investigated impartially, with appropriate corrective actions implemented where a breach is identified. The complainant is informed in writing of the outcome and any actions taken to address the issue.

- Where a privacy complaint cannot be resolved internally to the satisfaction of the individual, IOIS provides the complainant with the relevant **contact details for the Office of the Australian Information Commissioner (OAIC)** and information on how to escalate the matter externally. IOIS cooperates fully with any external review or investigation and implements required recommendations to strengthen privacy practices.

## 5. Responsibilities

- Clear responsibilities are assigned to ensure that personal information is managed lawfully, securely, and consistently across IOIS operations.
- The Chief Executive Officer (CEO) is responsible for ensuring that IOIS complies with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). This includes ensuring that appropriate policies, systems, and resources are in place to support effective privacy management and compliance.
- The Academic Manager (RTO Manager) is responsible for overseeing data management practices within IOIS. This role includes ensuring that personal information is collected, used, and disclosed in accordance with this policy, approving any external disclosures of personal information where required, and monitoring compliance with privacy obligations across training and assessment operations.
- The Administration and Student Support Officer is responsible for the day-to-day management of personal information. This includes collecting, storing, updating, accessing, and securely disposing of personal data in accordance with approved procedures, maintaining accurate records, and ensuring that privacy requirements are applied consistently in administrative and student support activities.
- Trainers and Assessors are responsible for protecting student confidentiality during training and assessment activities. This includes handling assessment evidence and student information securely, limiting access to authorised purposes only, and ensuring that personal information is not disclosed inappropriately during delivery, assessment, or feedback processes.

## 6. Related Documents

- Student Handbook
- Staff Handbook
- Enrolment Form
- Student Support Policy
- Complaints and Appeals Policy
- Records Management Procedure

Institute of International Studies (IOIS)
ABN: 86636830263 RTO: 45883
Address: Suite 703, Level 7, 79 George Street
Parramatta, NSW-2150
https: www.iois.edu.au

# Document Version Control

| | |
|---|---|
| Document Title | IOIS Privacy Policy and Associated Procedures |
| Reviewed By | Compliance Manager |
| Approved By | Chief Executive Officer |

| Version | Changelog | Created / Modified Date |
|---|---|---|
| 1.0 | IOIS Privacy Policy and Associated Procedures *V1.0* | July 2025 |