Privacy and Confidentiality Policy

CRICOS Code: 03638D

Document Control

Document Title	Privacy and Confidentiality Policy
RTO Code	45232
CRICOS Code	03638D
Document Owner	Operations Manager
Approved By	Chief Executive Officer
Version Number	2.0
Effective Date	20/08/2025
Next Review Date	20/03/2027
Related Documents	Domestic Student Handbook; International Student Handbook; International Admissions Policy and Procedure; PRISMS Management and Use Policy; Complaints and Appeals Policy; Student Support and Welfare Policy and Procedure; Continuous Improvement Policy; Data Breach Response Procedure; Information Security and Acceptable Use Procedure; Records Management and Retention Schedule

1. Purpose

This policy sets out how INT College collects, holds, uses, discloses, secures, corrects and destroys personal information and sensitive information in a way that is lawful, transparent and fit for purpose.

The policy is designed to support compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Student Identifiers Act 2014 (Cth), the National VET Data Policy, the ESOS Act 2000 and National Code 2018 for overseas students, and the 2025 Standards for Registered Training Organisations (RTOs).

2. Scope

This policy applies to all personal information and sensitive information handled by INT College in connection with its operations as an RTO and CRICOS provider, including information relating to prospective students, current students, former students, staff, contractors, agents, employers, education partners, placement hosts, complainants, witnesses and other stakeholders.

It applies across all campuses, delivery sites, online systems, student management systems, learning management systems, marketing systems, finance systems, PRISMS activity, USI processes, AVETMISS reporting processes and archived records.

For clarity, this policy applies to INT College operations at both the St Marys and Dubbo campuses and should be read consistently with the current Domestic Student Handbook, International Student Handbook and other related student-facing documents.

3. Legislative and Regulatory Framework

INT College manages privacy and confidentiality in accordance with applicable legislation, regulatory instruments and sector requirements, including where relevant:

- Privacy Act 1988 (Cth) and the 13 Australian Privacy Principles (APPs).
- Student Identifiers Act 2014 (Cth) and related requirements issued by the Student Identifiers Registrar.
- National Vocational Education and Training Regulator Act 2011 (Cth).
- National Vocational Education and Training Regulator (Outcome Standards for Registered Training Organisations) Instrument 2025.
- National Vocational Education and Training Regulator (Compliance Standards for NVR Registered Training Organisations and Fit and Proper Person Requirements) Instrument 2025.
- National VET Data Policy and Data Provision Requirements.
- Education Services for Overseas Students Act 2000 (Cth) and the National Code of Practice for Providers of Education and Training to Overseas Students 2018.
- Any applicable state or territory funding contracts, government program guidelines and recordkeeping obligations.

4. Policy Statement

INT College is committed to protecting privacy, maintaining confidentiality, and handling personal information fairly, lawfully and respectfully.

INT College will only collect information that is reasonably necessary for its functions and activities or otherwise required or authorised by law.

INT College will take reasonable steps to ensure individuals understand why information is being collected, how it will be used, who it may be disclosed to, and how they can access or correct it or make a complaint.

INT College will maintain systems, practices and controls appropriate to the nature of the information it holds and the risks associated with misuse, loss, unauthorised access, interference, modification or disclosure.

5. Definitions

Personal information: 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.

Sensitive information: Includes information such as health information, disability information, racial or ethnic origin, criminal record information and biometric information, as defined or treated under privacy law.

Government related identifier: A government-issued identifier such as passport details, visa details, Medicare details, concession details, tax file number or similar identifier.

APPs: The Australian Privacy Principles in Schedule 1 to the Privacy Act 1988 (Cth).

AVETMISS: Australian Vocational Education and Training Management Information Statistical Standard.

NCVER: National Centre for Vocational Education Research Ltd.

DEWR: Australian Government Department of Employment and Workplace Relations, including responsibilities connected with National VET Data settings and policy.

USI: Unique Student Identifier.

PRISMS: Provider Registration and International Student Management System.

6. Roles and Responsibilities

Chief Executive Officer - Approves this policy, ensures resourcing and oversight, and promotes a culture of lawful and ethical information handling.

Operations Manager (Privacy Contact) - Acts as the primary contact for privacy enquiries, access and correction requests, complaints, breach notifications and internal guidance.

Management team - Implements privacy controls, monitors compliance, manages risks, approves disclosures where required, and ensures third-party arrangements address privacy obligations.

Staff, trainers, assessors and contractors - Must only access and use information for authorised work purposes, maintain confidentiality, follow this policy, report incidents promptly and complete relevant training.

Agents and third-party service providers - Must handle information only in accordance with approved contracts, directions and applicable privacy obligations.

7. Information Collected

Depending on the person's relationship with INT College, the College may collect and hold information including:

- Identity and contact details, date of birth, emergency contacts and next of kin details
- Enrolment, attendance, academic progress, participation, support needs, complaints, appeals and outcomes
- USI information, visa information, passport details, citizenship or residency status and CRICOS/PRISMS related information
- Language, literacy and numeracy information, disability or medical information where relevant to support, safety or reasonable adjustment
- Work placement, employer, referee and workplace supervisor information
- Financial and billing information, payment history and government funding eligibility details
- Employment and contractor information including qualifications, right to work, payroll, superannuation and background screening information where relevant and lawful
- Website, enquiry, marketing preference and system usage information
- Student welfare, wellbeing, counselling referral, support meeting, intervention, attendance and action plan records created to support the student during their enrolment
- Contact update records, including changes to residential address, phone number, email and emergency contact details

8. How Information is Collected

INT College generally collects information directly from the individual through application and enrolment forms, pre-training reviews, student support interactions, assessments, surveys, interviews, emails, phone calls, websites, portals, learning platforms and other business processes.

Information may also be collected from a third party where the individual has consented, where collection is reasonably necessary for delivery or support, or where collection is required or authorised by law. This may include employers, education agents, referees, placement hosts, government agencies, the USI Registrar, authorised representatives or support persons.

Examples include trainer observations, attendance records, placement feedback, support notes signed or acknowledged by the student, and information provided by authorised staff involved in welfare, academic progress, finance or compliance management.

Where INT College receives unsolicited personal information, it will assess whether it could lawfully have collected that information. If not, and if lawful and reasonable to do so, INT College will de-identify or securely destroy it.

9. Purposes of Collection, Use and Disclosure

INT College uses and discloses personal information only for the primary purpose for which it was collected, for related secondary purposes that would reasonably be expected, with consent, or as otherwise required or authorised by law.

Typical purposes include:

- Assessing enquiries, applications, suitability, entry requirements and eligibility
- Delivering training, assessment, learner support, wellbeing support and reasonable adjustment
- Maintaining academic, administrative, financial and student support records
- Issuing AQF certification documentation and responding to replacement requests
- Meeting obligations under the Standards for RTOs 2025, the National VET Data Policy, AVETMISS, funding contracts, the ESOS framework, PRISMS and other legal requirements
- Communicating with students, staff, employers, agents, placement hosts and authorised representatives
- Responding to incidents, complaints, appeals, audits, regulators, litigation, law enforcement requests or health and safety matters
- Documenting student support interactions, intervention strategies, welfare referrals and agreed action plans, and sharing those records only with staff who have a legitimate operational need to know
- Maintaining up-to-date student contact details so INT College can communicate important information about enrolment, training, assessments, support services and student safety
- Undertaking quality assurance, continuous improvement, internal audits, risk management and business operations

10. Regulatory and Required Disclosures

As an RTO and CRICOS provider, INT College is required to disclose certain information to regulators, government departments and authorised bodies. Depending on the circumstances, this may include disclosure to ASQA, NCVER, DEWR, state or territory training authorities, the USI Registrar, PRISMS, the Department of Education, Home Affairs-related processes, auditors, funding bodies and other entities authorised by law.

INT College will include the current National VET Data Privacy Notice in enrolment processes where required and will ensure students are informed that personal information may be disclosed for statistical, administrative, regulatory and research purposes in accordance with sector requirements.

INT College may also disclose information to employers, workplace supervisors, education agents, government agencies, support services, emergency contacts or authorised representatives where this is lawful, necessary and proportionate.

Student welfare and support information will only be shared internally on a need-to-know basis, for example with relevant management staff where required for the student's wellbeing, safety, support coordination, serious matters or lawful decision-making.

11. Overseas Students and ESOS-Specific Requirements

For overseas students, INT College handles personal information in a way that supports compliance with the ESOS Act 2000, National Code 2018 and CRICOS obligations.

International students must notify INT College of changes to their residential address, mobile number, email address and emergency contact details within 7 days, and INT College will maintain and update these records in accordance with ESOS requirements.

INT College may collect, use and disclose information necessary to manage enrolment, course variations, attendance or progress intervention, student support, wellbeing matters, PRISMS reporting and other visa-related obligations.

This may include information used to monitor attendance, course progress, intervention strategies, deferment or suspension requests, withdrawals, CoE status and release or reporting actions recorded through PRISMS where required by law.

12. Direct Marketing and Communications

INT College will not sell personal information to third parties.

Marketing communications will only be sent where permitted by law and, where required, with consent. Individuals will be provided with a simple opt-out mechanism for non-essential communications.

Operational, compliance, student support and safety communications are not considered direct marketing and may still be sent where necessary.

13. Anonymity and Pseudonymity

Where lawful and practicable, individuals may deal with INT College anonymously or by using a pseudonym, for example when making a general enquiry or anonymous feedback.

However, anonymity or pseudonymity will generally not be possible where INT College must verify identity or collect information to enrol a student, issue certification, create or verify a USI, report data, manage employment, investigate a complaint fairly, or comply with legal obligations.

14. Cross-Border Disclosure and Offshore Access

INT College will take reasonable steps to avoid disclosing personal information overseas unless the disclosure is authorised, necessary for approved operations, supported by consent, or otherwise permitted by law.

If approved offshore staff or service providers access information on behalf of INT College, the College will implement contractual, technical and organisational controls designed to protect that information and ensure handling remains consistent with Australian privacy obligations.

Where cloud or software providers are used, INT College will assess the service, the location of storage or support access where practicable, and the privacy/security terms applying to the arrangement.

Physical and electronic records containing personal information, including student files and support records, must be stored securely and accessed only by authorised personnel. Staff must not disclose or discuss confidential information outside authorised work purposes.

15. Data Quality

INT College will take reasonable steps to ensure personal information it collects, uses and discloses is accurate, up to date, complete and relevant.

Students and staff are expected to provide accurate information and to notify INT College promptly of any changes.

Records will be updated when errors are identified through routine review, student contact, staff notification, audit activity or correction requests.

16. Information Security and Confidentiality Controls

INT College will implement reasonable physical, administrative and technical safeguards appropriate to the sensitivity of the information and the risks involved.

These controls may include role-based access controls, password protection, multifactor authentication, secure backups, audit logs, locked storage, secure disposal, confidentiality clauses, staff induction and training, incident reporting and periodic review of user access.

Only authorised personnel may access personal information, and only to the extent needed to perform their duties.

Staff must not disclose confidential information to any unauthorised person inside or outside the organisation and must take care when discussing student or staff matters, including in classrooms, open offices, emails, messaging tools and phone calls.

17. Retention and Destruction of Records

INT College will retain records for the minimum periods required by law, regulation, funding contract or operational need, and will securely destroy or de-identify personal information when it is no longer required and lawful to destroy.

Without limiting the above, INT College will retain AQF certification issuance records for at least 30 years and completed assessment evidence for the period required under the Standards for RTOs and related regulatory instruments, unless a longer period is required by law or contract.

Without limiting the above, INT College will retain records of AQF certification documentation issued to VET students for 30 years and retain assessment evidence submitted by a VET student for at least 2 years after the student has completed the training product, unless a longer period is required.

Secure destruction may include cross-cut shredding of hard copy records and secure electronic deletion or destruction of digital records.

18. Access to and Correction of Personal Information

Individuals may request access to their personal information held by INT College and may request correction of information they believe is inaccurate, out of date, incomplete, irrelevant or misleading.

Requests should be made in writing to the Operations Manager as the nominated Privacy Contact. INT College may take reasonable steps to verify identity before granting access or making a correction.

INT College will respond within a reasonable period and, where access is refused, will provide written reasons to the extent required by law and explain available complaint options.

Where appropriate, access may be provided by supervised inspection of the relevant student file or by providing copies of records, subject to lawful limitations, identity verification, reasonable administrative arrangements and any applicable authorised fees for copies or replacement documents.

INT College will not charge a fee for making a request, but may charge reasonable administrative costs for extensive copying, printing or postage where permitted.

19. Privacy Complaints

Any person who believes INT College has mishandled their personal information or breached this policy may make a privacy complaint.

Complaints should be submitted in writing to the Operations Manager as the nominated Privacy Contact. INT College will acknowledge receipt, assess the complaint, investigate it in a fair and timely manner, and provide a written outcome.

If the complainant is dissatisfied with the outcome, INT College will advise them of any available internal review pathway and, where relevant, their right to raise the matter with the Office of the Australian Information Commissioner or another appropriate external body.

Where a complainant is dissatisfied with INT College's response, they may be advised of external review options, including the Office of the Australian Information Commissioner, ASQA or other relevant agencies depending on the issue.

20. Eligible Data Breaches and Incident Management

INT College will respond promptly to actual or suspected privacy incidents, including loss, unauthorised access, unauthorised disclosure or other compromise of personal information.

Incidents will be escalated to authorised management for assessment, containment, investigation, remediation and documentation.

Where INT College has reasonable grounds to believe an eligible data breach has occurred, it will comply with applicable notifiable data breach obligations.

21. Website, Cookies and Online Services

INT College may collect limited online information such as IP address, browser type, pages visited, form submissions and cookie-related information for website functionality, analytics, security and service improvement.

Online payment or form systems used by INT College must be appropriately secured. Third-party platforms may also collect information in accordance with their own privacy terms.

22. Related Documents

This policy should be read together with related enrolment, student support, complaints and appeals, data reporting, staff conduct and continuous improvement documents, as well as the current Domestic Student Handbook and International Student Handbook.

Associated procedures and schedules may set out practical steps for privacy notices, identity verification, record access, correction requests, PRISMS handling, AVETMISS/NCVER reporting, USI processing, breach response, information security and secure destruction.

23. Privacy Contact

Privacy Contact: Operations Manager

Email: shivana@int.edu.au

Phone: 1800 046 846

Postal address: 5/40 Phillip St, St Marys, NSW, 2760