



Privacy and Personal Information Policy

Australian Institute of Digital Technology Pty Ltd

Version 2.0 | Effective 1 June 2026

RTO
45801

CRICOS
03983J

ABN
70 643 935 586

Level 1, 377 Lonsdale Street, Melbourne VIC 3000
support@aidt.edu.au | 0411 441 061 | www.aidt.edu.au



POLICY 10

Privacy and Personal Information Policy

Document Number	AIDT-POL-010	Version	2.0
Effective Date	1 June 2026	Next Review Date	June 2027
Policy Owner	CEO	Approved By	CEO
Applicable Legislation & Standards	Privacy Act 1988 (Cth) — Australian Privacy Principles 1–13; ESOS Act 2000 (ss.19, 26A); National Vocational Education and Training Regulator Act 2011; Student Identifiers Act 2014; NCVER Data Provision Requirements 2023; Health Records Act 2001 (Vic)		

1. Purpose and Commitment

AIDT is committed to protecting the privacy and confidentiality of all personal information it collects, holds, uses, and discloses in the course of its operations as a CRICOS-registered provider and registered training organisation. This policy sets out how AIDT handles personal information in compliance with the Privacy Act 1988 (Cth) and the thirteen Australian Privacy Principles (APPs). It applies to the personal information of students, staff, agents, and any other individual whose information AIDT collects.

For international students, privacy protections are particularly significant. Many students are sharing sensitive personal information — visa details, health information, financial details, address information — with an institution they have only recently met, in a country whose legal framework they may not fully know. AIDT's privacy obligations are a concrete expression of the trust students place in AIDT when they enrol. This policy is designed to ensure that trust is honoured in practice, not just on paper.

This policy acknowledges that some of AIDT's information sharing obligations are mandatory and cannot be declined. Specifically, AIDT is legally required to share certain information with the Department of Home Affairs, NCVER, ASQA, and the USI Registrar. These obligations are set out transparently in this policy so that students understand, before they enrol, what will and will not be kept confidential.

2. Personal Information AIDT Collects

AIDT collects personal information that is reasonably necessary for its functions as an education provider and a CRICOS provider. It does not collect personal information beyond what is genuinely necessary. The categories of personal information collected include:

- **Identity and contact information:** Legal full name, preferred name, date of birth, gender (for statistical reporting), nationality, country of birth, passport number, Australian residential address, mobile phone number, and email address. Emergency contact details (name, relationship, phone) for both Australian and overseas contacts.
- **Academic and enrolment records:** Qualification code and title, units of competency enrolled in, assessment task results, attendance records, course progress status, LLND assessment results, Student Support Plan contents,



- Reasonable Adjustment Plan contents, and all qualification and certification data.
- **Visa and immigration information:** Student Visa subclass, visa grant number, visa grant date, visa expiry date, CoE number, CoE dates, and any PRISMS reporting events recorded during the student's enrolment.
 - **Financial information:** Tuition fee invoices and payment records, refund applications and outcomes, and bank account details provided for refund processing. AIDT does not store credit card or banking login credentials.
 - **Unique Student Identifier (USI):** Collected, verified, and stored as required by the Student Identifiers Act 2014.
 - **Health and disability information:** Voluntarily disclosed health or disability information relevant to a Reasonable Adjustment request or welfare support referral. This is sensitive information under the APPs and is held with the highest level of confidentiality. AIDT does not require disclosure of health information as a condition of enrolment.
 - **Cultural and linguistic background:** Collected for AVETMISS statistical reporting and for the facilitation of culturally appropriate student support. Disclosure is voluntary.

3. How and Why Information Is Collected

AIDT collects personal information directly from the individual wherever practicable — through the Application for Enrolment Form, the Written Student Agreement, the LLND assessment, orientation processes, and ongoing course administration. Where information is collected from third parties — such as education agents, placement host supervisors, or previous training providers — AIDT takes steps to ensure the individual is either notified of the collection or was aware of it at the time.

AIDT collects personal information only for purposes that are directly connected with its functions as an RTO and CRICOS provider. These purposes include: processing and managing enrolments; delivering training and assessment; issuing AQF qualifications and records of results; monitoring course progress and attendance; administering fees and refunds; complying with mandatory reporting obligations under the ESOS Act, NVETR Act, and National Code; providing academic and welfare support services; and participating in government statistical and regulatory data collections.

AIDT does not collect personal information for marketing purposes beyond what is required to manage its relationship with enrolled and prospective students. AIDT does not sell, rent, or share student personal information with commercial third parties.

4. Mandatory Disclosures to Government and Regulatory Bodies

Several of AIDT's information-sharing obligations are not optional — they are legally mandated, and students cannot prevent or delay them by withholding consent. AIDT is transparent about these obligations because informed students are better positioned to understand and comply with their own regulatory obligations. The mandatory disclosures are as follows:



Department of Home Affairs (DHA) — via PRISMS	Mandatory under the ESOS Act 2000. AIDT reports: enrolment commencement, changes, suspension, and cancellation; unsatisfactory course progress reports (following the full ITR process); and address updates. Students are notified of each PRISMS report as it is made.
NCVER — AVETMISS data submission	Mandatory under the NVETR Act 2011 and NCVER Data Provision Requirements. Annual submission of training activity data including: student identity and demographics; enrolment details; units completed; assessment results; and employment and qualification status. NCVER's handling of this data is governed by its own Privacy Policy (www.ncver.edu.au/privacy).
Australian Skills Quality Authority (ASQA)	ASQA has the right to access AIDT's student records, training files, and assessment documentation during audits, registration reviews, and compliance monitoring under the NVETR Act.
USI Registrar	AIDT reports qualification completions and verifies USIs as required by the Student Identifiers Act 2014. AIDT does not disclose a student's USI transcript to any third party without the student's explicit written permission.
Tuition Protection Service (TPS)	AIDT provides enrolment and financial data to the TPS as part of its provider participation obligations.
Emergency Services	Personal information is disclosed to emergency services where necessary to protect the life, health, or safety of the student or another person. This disclosure does not require consent.

5. Data Security

AIDT takes the security of personal information seriously and implements technical and physical controls proportionate to the sensitivity of the information held. Electronic records are stored in AIDT's student management system with: strong password requirements for all staff access; role-based access controls so that each staff member can only access the data their role requires; audit logging of access and changes; and regular security reviews. Paper records containing personal information are stored in locked filing cabinets at AIDT's campus, with access restricted to staff with a legitimate need.

Where personal information is transmitted electronically — for example, in correspondence with ASQA, NCVER, DHA, or education agents — AIDT uses secure email or encrypted file transfer methods. Staff members do not email sensitive personal information (passport copies, health records, financial information) through unsecured channels.

6. Retention and Disposal

AIDT retains personal information for the minimum period required by law and then securely destroys it. The following retention periods apply:



Qualification and certification records	Minimum 30 years (Standards for RTOs 2025).
Enrolment and academic records	Minimum 7 years.
Financial and fee records	Minimum 7 years (consistent with ATO requirements).
Complaints and appeals records	Minimum 5 years.
LLND assessment records	Minimum 7 years.
PRISMS reporting records	Minimum 7 years or until resolution of any related regulatory matter.
Health and disability information	Minimum 7 years (Health Records Act 2001 (Vic)).

At the end of the applicable retention period, paper records are cross-shredded and electronic records are permanently deleted using approved data erasure software. Records subject to a pending legal proceeding or regulatory investigation are not destroyed until that matter is resolved, regardless of the standard retention period.

7. Access, Correction, and Privacy Complaints

Under Australian Privacy Principles 12 and 13, individuals have the right to access the personal information AIDT holds about them and to request correction of any information that is inaccurate, out of date, incomplete, or misleading. Access requests must be submitted in writing to privacy@aidt.edu.au. AIDT responds within 30 calendar days. AIDT does not charge for responding to access requests.

Correction requests are also submitted in writing. AIDT corrects information found to be inaccurate within 10 business days. Where AIDT declines a correction request, it provides written reasons and notes the existence of the correction request on the relevant record.

Privacy complaints are handled through AIDT's Complaints and Appeals process (AIDT-POL-009). Where an internal complaint does not resolve the matter, the individual may escalate to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or 1300 363 992.