

# PP33 – Student identifier management policy

## 1. Purpose

This policy ensures that AEATS complies with Clause 12 of the Standards for RTOs and the Student Identifiers Act 2014 by managing the collection, verification, protection, and use of Unique Student Identifiers (USIs) in a secure and lawful manner.

## 2. Scope

This policy applies to all staff and students involved in the collection, use, and storage of student USIs.

## 3. Definitions

Term	Definition
USI (Unique Student Identifier)	A 10-digit alphanumeric reference assigned to each VET student in Australia.
AVETMISS	The Australian Vocational Education and Training Management Information Statistical Standard, which requires valid USIs for national reporting.
Registrar	The national authority responsible for administering the USI system.

## 4. Legislative and Regulatory References

- Student Identifiers Act 2014
- Student Identifiers Regulation 2014
- Privacy Act 1988
- Standards for RTOs 2025 – Clause 12
- Data Provision Requirements 2012

## 5. Policy Statement

AEATS ensures:

- All students are informed of the USI requirement before enrolment.
- USIs are collected and verified before issuing any AQF certification documentation.
- No training activity is reported to NCVER unless a verified USI is present.
- Personal information used for USI access is collected, stored, and used in accordance with the Privacy Act.

## 6 Step-by-Step Procedure – Student Identifier Management

Step	Action	Responsible Person
1	<b>Collect Personal Information and Consent-</b> The enrolment form collects the students personal information, USI, training records, and other relevant data from the student.- The student sign's consent for data collection and usage as per the Privacy Act and AEATS policies at the bottom of the enrolment form.	Enrolment Officer
2	<b>Secure Data Storage-</b> Enter student and training data into secure systems, including the Student Management System (SMS), financial software (e.g. Xero). Restrict access to authorised personnel only using role-based permissions.	Enrolment Officer / Business Manager
3	<b>Maintain Register of Issued Qualifications-</b> Keep a centralised register of all AQF qualifications and Statements of Attainment issued.- Ensure records align with AQF Qualifications Register Policy.- Records must include student name, USI, qualification code/title, date issued.	Business Manager/ Compliance Manager
4	<b>Retention of Enrolment Records-</b> Store enrolment forms and supporting evidence (e.g. ID, LLND results) for 7 years from completion or withdrawal.	Enrolment Officer
5	<b>Retention of Financial Records-</b> Retain student payment records, invoices, refund processing documentation, and transaction summaries for 7 years, in line with ATO and audit requirements.	Business Manager
6	<b>Retention of Complaints and Appeals Records-</b> Keep copies of submitted complaints and appeals, outcome letters, investigation records, and resolution documentation for 5 years.	Compliance Manager
7	<b>Retention of Assessment Evidence (Including RPL)-</b> Retain all assessment evidence (e.g. completed workbooks, observation checklists, assessor marking tools, validation records) for 2 years after the student's completion of the qualification or standalone unit. <ul style="list-style-type: none"> <li>For RPL, retain application forms, RPL mapping documents, evidence submitted (certificates, work samples), assessor's final judgment, and RPL outcome communication.</li> </ul>	Managing Director

Step	Action	Responsible Person
	<ul style="list-style-type: none"> <li>Ensure electronic copies are kept in the student's digital file on dropbox or the LMS where applicable.</li> </ul>	
8	<b>Access to Records Upon Request-</b> If a student or former student requests access to their records (e.g. certificate reissue, attendance records), provide access or copies within 4 weeks.- Log all requests in the Access Request Register. Requests must be in writing and sufficient identification required. Must be approved by the Compliance Manager.	Compliance Manager
10	<b>Secure Disposal of Expired Records-</b> Once minimum retention periods are met: - Shred physical documents. - Permanently delete electronic records from all storage systems.- Disposal must be authorised and recorded on a Destruction Log.	Compliance Manager

### 7. Privacy & Consent

USIs and personal data collected for verification are handled under the Australian Privacy Principles (APPs). Consent for USI creation or access must be recorded through the enrolment form or via written authorisation.

### 8. Third Party Obligations

Any third party involved in training delivery or student recruitment must comply with this policy and maintain confidentiality of USI information.

### 9. Breach and Compliance

Failure to comply with this policy may result in:

- Withholding of AQF documentation;
- Breach reporting to the Registrar;
- Disciplinary action for staff or third parties.

### 10. Related Documents

- enrolment forms
- Student Management System (SMS)
- Certification Register (VETtrak)