PP34 – Data privacy and record keeping policy

1. Purpose

This policy ensures that AEATS manages student and staff records in a manner that protects personal information, meets legislative data privacy obligations, and aligns with Clause 10 of the Standards for RTOs 2025. The policy also ensures that record keeping practices support transparency, accuracy, and regulatory compliance.

2. Scope

This policy applies to:

- All personal and training records of students
- AEATS staff, contractors, and third parties who handle personal or sensitive information
- Storage, access, and disposal of physical and digital records

3. Definitions

Term	Definition
Personal Information	Information or opinion that identifies or could identify an individual (e.g., name, address, date of birth, USI)
Sensitive Information	A subset of personal information including health, disability, racial background, or religious beliefs
AVETMISS	The data standard used to collect VET sector data
NCVER	National Centre for Vocational Education Research
USI	Unique Student Identifier – mandatory for all nationally recognised training

4. Legislative References

- Standards for RTOs 2025 – Clause 10
- National Vocational Education and Training Regulator Act 2011
- Australian Privacy Principles (Privacy Act 1988)
- Archives Act 1983
- Data Provision Requirements 2020
- AVETMISS and USI Reporting Requirements

5. Policy Statement

AEATS is committed to:

- Protecting the privacy of personal and sensitive information it collects
- Meeting all legislative requirements for the retention, storage, and security of records
- Ensuring students have access to their records upon request
- Retaining training and assessment records for at least 30 years
- Retaining other required records (e.g., complaints, appeals, enrolment records) for a minimum of seven years, or as otherwise legally required
- Implementing strict access controls and secure disposal practices

6. Procedure – Step-by-Step

Step	Action	Responsible Person	Timing
1	Collect personal information only where necessary (e.g., enrolment, LLN, AVETMISS, USI)	Enrolment Officer	At enrolment
2	Ensure all personal data is collected with consent and privacy notice is provided. This is collected via the enrolment form.	Enrolment Officer	During enrolment
3	Store physical records in locked cabinets, then the AEATS official document storage. Digital records are stored in password-protected systems with backups	All staff	Ongoing
4	Provide students access to their personal and training records upon written request	Compliance Manager	Within 10 business days
5	Regularly review access controls and restrict data handling to authorised staff only	Managing Director	Quarterly
6	Back up digital data daily and store backups securely in a secure cloud	Managing Director	Daily
7	Archive training and assessment records securely for 30 years	Managing Director	Ongoing
8	Retain financial, complaint, appeal and enrolment records for 7 years minimum	Managing Director	Ongoing

Step	Action	Responsible Person	Timing
9	Securely dispose of expired paper records by shredding or certified destruction. Enter record in document destruction log.	Managing Director	As required
10	Ensure all staff have signed the Staff Confidentially Agreement on data privacy responsibilities and breach response.	Compliance Manager / Managing Director	At induction
11	Report any data breaches to the Managing Director and investigate in line with the Notifiable Data Breaches Scheme	All staff	As required

7. Related Documents

- Student Enrolment Form
- Privacy Notice
- Access to Records Request in writing
- Data Breach Response Plan
- Complaints, Appeals and Compliments Register
- Records Management Procedure
- AEATS Data Retention
- Staff Confidentiality Agreement