PP47 – Privacy policy

1. Purpose

This policy outlines how AEATS collects, uses, discloses, stores, and protects personal information in accordance with the Privacy Act 1988, including the Australian Privacy Principles (APPs). The policy ensures AEATS staff and students understand their privacy rights and the organisation's responsibilities in managing personal and sensitive data.

2. Scope

This policy applies to all AEATS personnel, students, and third parties who handle or access personal or sensitive information relating to VET operations, including during enrolment, training, assessment, and support services.

3. Definitions

Term	Definition
Personal Information	Information that identifies or can reasonably identify an individual (e.g., name, address, phone number, email, USI).
Sensitive Information	Information such as health status, racial/ethnic origin, disabilities, and other data requiring a higher level of protection.
APPs	Australian Privacy Principles outlined under the Privacy Act 1988.
Data Breach	When personal information is accessed, disclosed, or lost in an unauthorised or accidental manner.

4. Legislative References

- Standards for RTOs 2025 – Clause 20
- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- National VET Data Policy
- Student Identifiers Act 2014

5. Policy Statement

AEATS is committed to protecting the privacy and confidentiality of all individuals' personal and sensitive information. AEATS will:

- Collect only necessary information relevant to enrolment, training, support, and compliance;
- Inform individuals about the purpose of collection and how their data will be used;
- Obtain written consent before sharing data with third parties unless required by law;

- Ensure records are stored securely and retained in accordance with regulatory obligations;
- Respond to privacy complaints or requests to access personal data within 10 business days.

6. Collection and Use of Information

- Information is collected during the pre-enrolment and enrolment process, including via the Enrolment Form, email and phone conversation.
- **Data collected may include:**
    - Identity details (e.g., name, date of birth)
    - Contact details
    - USI
    - Emergency contact details
    - Health or disability disclosures (with consent)
    - Citizenship/visa status
- **This data is used to:**
    - Provide training and assessment
    - Manage student records
    - Comply with AVETMISS and other government reporting
    - Issue AQF certification

7. Storage and Security

All personal data is stored securely using:

- Student Management System (SMS) for enrolment and academic records
- Encrypted cloud storage for administrative files
- Access control protocols to restrict data to authorised staff
- Backups and IT security measures to protect electronic files

8. Disclosure

AEATS may disclose personal information to:

- Commonwealth and State Government departments
- NCVER and other regulatory bodies

No data will be sold or disclosed for marketing without permission.

9. Access and Correction

- Individuals may request access to their records by contacting the Admin Officer.
- Any incorrect or outdated personal information will be updated upon verification.

10. Breach Management

In the event of a suspected or confirmed privacy breach:

1. The Compliance Manager will conduct an immediate assessment.
2. Individuals affected will be notified if required.
3. The breach will be reported to the Office of the Australian Information Commissioner (OAIC), where applicable.

11. Procedure – Step-by-Step

Step	Action	Responsible Person
1	Collect personal and sensitive information at enrolment with consent.	Enrolment Officer
2	Store records in secure systems (SMS, Dropbox, finance tools).	Enrolment Officer
3	Restrict data access to authorised personnel.	Managing Director
4	Share data with government only with consent or as required by law.	Compliance Manager
5	Provide access to records upon student request form verification.	Enrolment Officer
6	Handle correction requests within 10 business days.	Enrolment Officer
7	Investigate and report data breaches promptly.	Compliance Manager
8	Induct staff on privacy principles.	Compliance Manager
9	Review policy every 12 months or after legislative change.	Compliance Manager

12. Related Documents

- Enrolment Form
- Student Handbook
- Privacy Consent via enrolment form
- Data Breach Response Plan
- PP34 - Data Privacy and Record Keeping Policy