Records, Privacy, and Document Control Policy

1. Purpose

To outline AA Academy's approach to managing records, ensuring privacy of personal information, and maintaining document control in line with Standards for RTOs 2015 (Clauses 3.4, 3.5, 4.1, 8.1) and in preparation for the Revised Standards 2025. This policy also supports compliance with the Privacy Act 1988 and the Student Identifiers Act 2014.

2. Scope

Applies to all student records, assessment evidence, learning and assessment materials, third-party agreements, internal policies, and organisational data managed by AA Academy.

3. Core Principles

3.1 Records Management

- A file is maintained for each student with enrolment, training, assessment, and certification records.
- AVETMISS and USI data are managed through the Student Management System (SMS).
- Certification records are retained for 30 years; all other records for at least 7 years.
- Obsolete student records and administrative files are securely archived or disposed of in accordance with data protection regulations.

3.2 Privacy and Confidentiality

- Personal data is collected lawfully and stored securely.

- Students provide informed consent at enrolment for the collection, use, and disclosure of their personal information, in accordance with the Australian Privacy Principles.
- Access to records is restricted to authorised staff.
- Students can request access to their records via a formal request, responded to within 10 business days.

3.3 Document Control and Versioning

- All policy and procedural documents, assessment tools, and training materials are subject to version control.
- Superseded versions are archived and removed from active access folders to prevent unintended use.
- Changes are logged, and current versions are stored securely in the RTO's shared governance folder.
- Documents are reviewed at least annually or as required.

3.4 Data Retention and Disposal

- Retention periods comply with legislative and regulatory requirements: 30 years for AQF certification records; 7 years minimum for general administrative records.
- Disposal is conducted using secure methods appropriate to the format: digital files are permanently deleted and physical records are shredded or destroyed securely.
- A disposal log is maintained for any destruction of records, including date, document type, and method of disposal.
- All staff must confirm that no active legal, audit, or compliance requirements apply before initiating disposal.

4. Procedures Summary

Step	Task	Responsible
1	File and update student records in SMS	Admin Officer
2	Backup digital records weekly	IT/Compliance Officer
3	Respond to student access requests	Admin Officer
4	Review and update policy versions	Compliance Manager

5	Submit AVETMISS and verify USIs	RTO Manager / Admin
6	Archive or dispose of outdated documents	Compliance Manager
7	Maintain disposal log and confirm no active obligations exist	Compliance Manager

5. Related Documents

- USI Access and Privacy Guide
- Version Register
- Student Record Request Form
- Document Review Log
- Data Retention and Disposal Guidelines
- Record Disposal Log Template