



ROYAL
INTERNATIONAL
COLLEGE

RTO Code: 46036 | CRICOS Code: 04153F

RECORDS MANAGEMENT POLICY AND PROCEDURE

☎ +61 0461414506 ☎ +61 491 138 564

🌐 www.royalinternational.edu.au

✉ support@royalinternational.edu.au

✉ admissions@royalinternational.edu.au

📍 **Melbourne** (Head Office)

Suite 2, Level 6, 341, Queen Street,
Melbourne VIC 3000 Australia

📍 **NSW** (2nd Campus)

406/2-8, Brookhollow Ave,
Norwest, NSW - 2153



Table of Contents

1.25. Records Management Policy and Procedure	3
Policy Content	3
Purpose	3
Objective	3
Scope	3
Policy Statement	4
General Principles	4
Procedures:	4
Roles and Responsibilities	7
Continuous Improvement	8
Confidentiality and Privacy	8
Review and Retention	9

1.25. Records Management Policy and Procedure

Policy Content

Aspect	Details
Regulator	Australian Skills Quality Authority (ASQA)
Standards Referenced	
Legislation / Requirements	

Purpose

The purpose of this policy is to ensure that all records created, received, and maintained by the RTO are managed securely, systematically, and in compliance with relevant legislative and regulatory requirements. This includes student records, training and assessment documentation, compliance evidence, and administrative data.

Objective

This policy aims to:

- Safeguard the accuracy, integrity, confidentiality, and accessibility of RTO records.
- Ensure retention, archiving, and disposal practices meet all legislative and regulatory requirements.
- Provide clear procedures for the creation, maintenance, storage, access, and destruction of records.
- Support audit readiness and demonstrate compliance with the Standards for RTOs 2025.

Scope

This policy applies to all staff, contractors, and third parties who create, access, or manage records on behalf of the RTO. It covers:

- Student records (enrolment, progression, completion, complaints)
- Training and assessment documentation

- Compliance and audit records
- Governance and operational records
- Digital and paper-based formats

Policy Statement

The RTO is committed to effective records management practices that:

- Comply with SRTO 2025, AVETMISS, ESOS (where applicable), and the Privacy Act
- Enable timely retrieval and secure storage of records
- Prevent unauthorised access, alteration, or destruction
- Ensure data accuracy and version control
- Facilitate evidence-based decision-making and continuous improvement

General Principles

- Records must be authentic, complete, reliable, and usable.
- All records must be stored securely for the minimum retention period as required by SRTO 2025.
- All student records related to competency decisions must be retained for a minimum of 2 years from the date the decision was made (Standard 10(c)).
- Electronic records must be backed up regularly and stored in controlled systems with appropriate security protocols.
- Access to records is restricted based on role responsibilities and governed by the RTO's Privacy Policy.
- Destruction of records must be authorised, documented, and conducted securely to protect confidentiality.

1.25.1 Procedures:

Step	Procedure	Details and Compliance Alignment
------	-----------	----------------------------------

1.25.1.1	Record Creation and Collection	All records must be generated at the time of the event or activity, including enrolment forms, assessment outcomes, validation minutes, attendance records, and complaints. Data must be accurate, dated, and signed by the relevant person.
1.25.1.2	Student Records Management	The RTO collects and maintains records of: - Student personal and contact information - Enrolment and USI data - Training participation and progress - Assessment outcomes and feedback - Qualifications issued (certificates and SoA) These must be securely retained for at least 2 years from the date the competency decision is made, per Standard 10(c).
1.25.1.3	Data Entry and System Use	All digital records are to be entered into the Student Management System (SMS) and Learning Management System (LMS). Staff must follow the system access protocols and ensure accuracy. Data is backed up regularly and protected by access controls.
1.25.1.4	Secure Storage and Access Control	Records must be stored securely in locked filing cabinets (physical) or encrypted databases (digital). Access is restricted to authorised personnel only, based on their role and responsibility. Privacy principles under the Privacy Act 1988 are enforced.
1.25.1.5	Retention and Archiving	The RTO retains: - Assessment evidence for 2 years from the competency decision

		- Financial and administrative records for 7 years - Enrolment and training records for at least 2 years Older records beyond retention limits are archived offsite or digitally in secure servers. A retention schedule is maintained.
1.25.1.6	Record Disposal and Destruction	Disposal of records occurs only after the minimum retention period. A destruction request must be authorised by the Compliance Officer. Confidential information is destroyed using shredding (physical) or secure deletion (digital). A record of destruction is retained.
1.25.1.7	Audit and Review Readiness	All records must be retrievable in case of audit or ASQA request. The Compliance Officer will ensure readiness by checking record currency, completeness, and storage every 6 months. Spot audits are conducted quarterly.
1.25.1.8	Third-Party Record Management	Where a third party is involved, the RTO ensures through written agreement that all records are collected, stored, and managed in compliance with SRT0 2025 and the RTO's Records Policy. Regular review of third-party compliance is conducted.
1.25.1.9	Record Access Requests	Students and staff may request access to their records via formal written request. The RTO must respond within 10 business days and ensure secure access under privacy requirements.
1.25.1.10	Version Control and Document Management	All policy, procedural, and compliance documents must include version numbers, issue dates, and review history. Updated versions must

		be approved and distributed through the Quality System and archived appropriately.
--	--	--

Roles and Responsibilities

Role	Responsibility
PEO (Principal Executive Officer)	- Ensures organisational commitment to records management compliance. - Approves policy and oversees compliance with legislative and regulatory requirements including the <i>Standards for RTOs 2025</i>.
RTO Manager / Compliance Manager	- Oversees implementation of records management practices. - Monitors retention schedules, security protocols, and audit readiness. - Ensures proper storage, version control, and destruction protocols are followed. - Ensures AVETMISS and Quality Indicator data requirements are met.
Trainers and Assessors	- Maintain complete and accurate assessment records and attendance. - Submit records in accordance with retention and archiving requirements. - Ensure confidentiality of student data and secure handling of assessment materials.
Student Support Officers	- Maintain student files including enrolment, support, and communication records. - Facilitate access requests and ensure privacy in handling data.
Administration Staff	- Enter and update data in Student Management System (SMS).

	- Assist in secure storage, retrieval, and archiving of physical and digital records. - Follow access and version control procedures.
IT and System Administrators	- Implement secure digital storage solutions with backup and recovery functions. - Maintain access controls and security of databases housing student records.
Third-Party Providers (where applicable)	- Maintain and submit records to RTO as per third-party agreements. - Comply with all records retention, confidentiality, and access protocols as set out by the RTO and SRT0 2025.

Continuous Improvement

- Records management practices are reviewed annually as part of the RTO's Continuous Improvement Cycle.
- Feedback from internal audits, ASQA audits, staff input, and student feedback is used to:
 - Refine procedures for data collection, retention, and destruction.
 - Enhance system access, storage protocols, and document control.
- All improvements and changes are:
 - Logged in the Continuous Improvement Register (CIR).
 - Reported in monthly Quality and Compliance meetings.
 - Reflected in updated procedures with new version control.

Confidentiality and Privacy

- All records are managed in accordance with the *Privacy Act 1988*, ensuring that personal information is:
 - Collected only for the intended and lawful purposes of RTO operations.

- Accessed only by authorised personnel.
- Disclosed only where consent is provided or where required by law.
- RTO ensures students are informed about their rights regarding personal data through enrolment forms and privacy statements.
- Staff are trained in privacy compliance and must sign confidentiality declarations upon induction.
- Sensitive records (e.g., health, disability, support needs) are stored with restricted access.

Review and Retention

Document / Record Type	Minimum Retention Period	Justification / Compliance Standard
Student enrolment records	2 years after enrolment ends	SRT0 2025 - Clause 10(c)
Assessment records (including RPL)	2 years from date of competency decision	SRT0 2025 - Clause 10(c)
Issuance records (qualifications, SoA)	30 years (digital copy)	ASQA General Direction - Retention of Issuance Documentation
Financial records	7 years	Australian Taxation Office (ATO) requirements
Complaints and appeals	5 years	SRT0 2025 and ESOS 2018 Standard 10
Internal audit records	5 years	SRT0 2025 = Standard 4.4
Marketing and publication records	5 years from use	To demonstrate compliance with marketing obligations
Policies and procedures	Until superseded + 5 years	To support audit trails and version tracking