

RECORDS MANAGEMENT POLICY & PROCEDURE

Introduction

The Kings Own International College (KOIC) is committed to the secure, accurate and lawful management of all records generated through its training, assessment, student-support and governance activities. Robust records management safeguards personal information preserves the integrity of KOIC's operations and provides the evidence base for transparent decision-making and continuous improvement.

This policy sets out KOIC's principles and procedures for creating, storing, accessing, archiving and disposing of records while protecting privacy and confidentiality. All activities are conducted in line with:

- Privacy Act 1988
- National Vocational Education and Training Regulator Act 2011 (including Clauses 7, 11, 12 and 14)
- Standards for Registered Training Organisations 2025 — Standards 1.3, 1.4, 1.8, 2.1, 2.2, 2.7, 4.1, 4.3 and 4.4
- Education Services for Overseas Students (ESOS) Act 2000 and National Code of Practice 2018; Standards 2, 3, 6, 7, 8, 9, 10, 11
- ELICOS Standards 2018
- Data Provision Requirements 2020
- Student Identifiers Act 2014

By adhering to these instruments KOIC ensures that every record—whether relating to students, staff, training products or corporate governance—is retained for the required period, remains verifiable and confidential, and is readily accessible to support regulatory reporting and organisational accountability.

Purpose

This Records Management Policy and Procedure ensures that KOIC maintains complete, accurate, secure, and accessible records and documents in compliance with all regulatory requirements. It supports the integrity of operations, student outcomes, governance obligations, and regulatory reporting.

Scope

This policy applies to all records and documents created or received in the course of KOIC's operations, including but not limited to:

- Personal, academic, and financial records of students enrolled in VET and ELICOS programs.
- Trainer qualifications and PD logs
- Enrolment and support documentation
- Certification issuance and validation records
- Learning and assessment tools
- Policies, procedures, templates, and forms
- Document registers, governance records, and review logs
- Records maintained for compliance with the *Privacy Act 1988*, *National Vocational Education and Training Regulator Act 2011*, and *ESOS Act 2000*.
- Systems used for the collection and management of student information, including the Student Management System (SMS) and hard copy records.

Policy Statement

Effective records and document management is critical to KOIC's ability to demonstrate compliance, manage risk, support transparency, protect student information, and ensure the integrity of training and assessment systems. This policy ensures records and documents are properly maintained, version-controlled, and reviewed throughout their lifecycle.

Records will:

- Be accurate, complete, current, and retained for the legally required duration,
- Be version-controlled and identifiable through structured naming conventions and registers,
- Be stored securely to prevent unauthorised access, loss, or damage,
- Be accessible only to authorised staff in accordance with role-based permissions,
- Be retrievable in a timely manner for internal, regulatory, or legal purposes,
- Be subject to regular audit and quality review, including lifecycle checks, integrity audits, and incident response reviews.

KOIC ensures that staff are trained in appropriate records management practices and that digital infrastructure supports data integrity, secure backups, and role-based system access. Governance of this policy is overseen by the Compliance Officer, and enforcement is the responsibility of all staff with access to regulated information.

KOIC recognises its additional recordkeeping obligations as a CRICOS provider under the National Code 2018, including maintaining written agreements, academic progress, transfer requests, and visa-related records for international students in accordance with Standards 2, 3, 6, 7, 8, 9, 10 and 11. For CRICOS-specific obligations, please refer to the CRICOS Addendum at the end of this document.

Definitions

Archiving	The secure transfer of inactive records into long-term storage from where they can be accessed for compliance, reissue, or audit purposes.
Assessment Tools	The structured materials used to collect evidence of competency. This includes task instructions, benchmarks, assessor guides, observation checklists, third-party reports, and assessment mapping.
AVETMISS	The Australian Vocational Education and Training Management Information Statistical Standard. It governs the consistent collection and reporting of VET enrolment and outcome data for national analysis.
Completed Student Assessment Items	Any student work and corresponding assessor records that demonstrate competency decisions. Includes completed assessment tasks, RPL documentation, practical assessment evidence, and assessor feedback.
Data Provision Requirements	The requirements for data provision as agreed by the Industry and Skills Council and implemented by the VET Regulator as required by its governing legislation.
NVR Act	National Vocational Education and Training Regulator Act 2011
Personal Information	Any information that identifies an individual, including their name, date of birth, contact details, and identification numbers

Privacy Act 1988	The Privacy Act 1988 is an Australian law that regulates the handling of personal information about individuals. It includes rules about how personal information is collected, used, stored, and disclosed, as well as access and correction rights for individuals.
Records	All documents and data, in any format (paper, digital, video, audio), created or received during the conduct of RTO operations, which serve as evidence of decisions, activities, or transactions.
Retention Period	The minimum period student records must be kept, as mandated by legislation.
Student Management System (SMS)	An AVETMISS-compliant system used to manage and store student data securely, including enrolment, progression, training delivery, outcomes, and certification.
Student Records	All records associated with a student's enrolment, learning, support, assessment, progress, complaints, and AQF certification. This includes both electronic and hard-copy records.
Transition Records	Documents required to demonstrate compliance with Clause 14 of the Compliance Requirements for RTOs 2025. Includes transition strategies, communication with students, mapping documentation, and evidence of teach-out or re-enrolment.
Unique Student Identifier (USI)	A unique 10-digit alphanumeric code assigned to each student undertaking nationally recognised training in Australia. The USI enables the creation of a lifelong training record and is verified through the national USI Registry.

Regulatory and Legislative Requirements

- Australian Privacy Principles
- Data Provision Requirements 2020
- ELICOS Standards 2018
- ESOS Act 2000
- ESOS National Code 2018
- NEAS Quality Assurance Framework
- NVR Act 2011
- Privacy Act 1988
- Standards for RTOs 2025; Quality Area 4: Governance, Outcome Standards 4.1 – 4.3, other relevant Outcome Standards include 1.3, 1.4, 1.8, 2.1, 2.2 & 2.7
- Compliance Requirements; Clauses 7, 11, 12 and 14

Records Management Procedure

KOIC maintains a centralised, secure, and accessible system of records and documents. All staff must use the current version of approved documents as recorded in the Document Management Register.

A. Document Control and Versioning

All documents are version-controlled using the convention: v0.1 (draft), v1.0 (initial approved), v1.1, v1.2 (minor amendments), v2.0 (major change).

Version details are recorded in the footer of every document along with approval date

B. Naming Convention

- [KOIC]_[Title]-[Version]-[Status] (e.g., KOIC_Assessment Policy v1.2 Final)
- No special characters
- Use underscores, and
- Version number.

C. Document Review and Approval

- Documents are reviewed at least annually or following legislative change, incidents,
- or continuous improvement outcomes.
- The Quality and Governance Calendar includes scheduled review dates. The Compliance Manager assigns a Reviewing Officer.
- The Reviewing Officer records all changes using a Document Review Record. CEO approval is required before publishing any updates.
- Updated documents are distributed to relevant staff, supported by training if necessary.

D. Document Storage and Access

- Documents are stored in structured digital folders with access restricted by role.
- Historical versions are archived. Backup protocols ensure data recovery.

E. Retention Period

KOIC applies clearly defined retention periods for each category of student and organisational records, based on legislative and regulatory requirements. These timeframes ensure the organisation meets its obligations under the Standards for RTOs 2025, the National Vocational Education and Training Regulator Act 2011, the Data Provision Requirements 2020, and, where applicable, the National Code 2018.

The following retention periods apply:

- Retained for a minimum of **30 years**, consistent with the requirement to maintain records of AQF certification documentation (Schedule 5 of the 2015 Standards still cited in guidance).
- Includes enrolment, participation, outcome results, and unit-level data entered into the Student Management System.

Written agreements (including refund calculations)

- Retained for a minimum of **2 years** after the student ceases to be an accepted student.
- Confirmation of Enrolment (CoE) and visa documentation **2 years** after enrolment date ends.

Completed Student Assessment Items

- Retained for a minimum of **2 years** from the date on which the judgment of competency was made.
- Applies to all forms of assessment evidence, including RPL documentation, third-party reports, practical assessments, and annotated student submissions.
- Records must be sufficient to demonstrate how the final assessment decision was made.

Assessment Tools

- Retained for a minimum of **5 years** from the last date the tool was used.
- Includes task instructions, benchmarks, assessment mapping, observation checklists, and marking rubrics.
- Used to verify assessment integrity and alignment with the training package or accredited course requirements.

Certification Records

- Records of AQF certification issued (including certificates and statements of attainment) are retained for **30 years**, stored securely within the SMS and backup archives.

Support, Progress, and Intervention Records

- Retained for a minimum of **2 years** after the student ceases to be enrolled.
- Includes support plans, progress monitoring, critical incidents, and records of any interventions

Administrative and RTO Management Records

- Documents relating to internal operations, such as versions of policies, procedures, registers, and governance records, are retained for a minimum of **5 years** unless otherwise specified.

CRICOS Specific Recordkeeping Requirements

- Applicable to all overseas student in accordance with the National Code 2018 (Standards 2 -11) and the ESOS Act 2000 are retained for a minimum period of **2 years** unless otherwise specified.

All retention periods are applied uniformly across physical and electronic records. Disposal of records must occur in accordance with KOIC's Retention and Disposal Schedule, following authorisation by the Compliance Officer or CEO. Where required, records are securely archived for long-term storage.

F. Archiving – Secure Transfer and Storage

KOIC applies structured processes for the archiving of both electronic and physical records once they are no longer active but must be retained for compliance, audit, or operational reference. Archiving practices are aligned with:

- the Compliance Requirements for RTOs 2025 (Clause 7),
- the Data Provision Requirements 2020,
- the Student Identifiers Act 2014, and

Electronic Records Archiving

- All student records within the Student Management System (SMS) are archived upon course completion or formal withdrawal.

- Archived records are digitally locked to prevent further editing and flagged as 'inactive.'
- The SMS and associated storage infrastructure must include:
 - Daily offsite or cloud-based backups,
 - Role-based access controls,
 - Version history retention,
 - Secure logins with multi-factor authentication.

Physical Records Archiving

- Where hard-copy assessment evidence, attendance sheets, or signatures are retained, documents are sorted by student ID, bundled, and clearly labelled.
- Hard-copy files must be stored:
 - In a lockable, fire-resistant, and pest-proof filing cabinet or off-site facility, and
 - In an area with restricted access, monitored by authorised personnel only.
- Records may be scanned for digital preservation using document scanning apps or MFDs (e.g., Scanner Pro, Adobe Scan) and stored in encrypted folders linked to the SMS.

1. Delivery and Handling Instructions

- Trainers and Assessors must submit finalised hard-copy records in an unsealed archive envelope, clearly marked with the student's name, course code, completion date, and assessor name.
- Records are either:
 - Hand-delivered to the Compliance Officer or
 - Sent via registered post with tracking to the designated storage location.
- Once received, administrative staff are responsible for:
 - Scanning, cataloguing, and assigning a file location,
 - Updating the Student Record Archiving Register,
 - Confirming with the assessor that the archiving process is complete.

2. Access to Archived Records

Archived records may only be accessed by authorised staff and must be signed in/out via the Archived Records Access Log. Any alterations or movement of physical files must be documented.

G. Record Lifecycle Management

- Student records (e.g. enrolment, USI, assessments) are stored securely and retained per legislative timeframes.
- Certification issuance records are retained for 30 years.
- Assessment tools and validation evidence are retained for at least 2 years post-assessment.
- Trainer files and PD logs are updated annually.
- All disposals are conducted by authorised personnel and documented in accordance with the approved Retention and Disposal Schedule
- In accordance with Clause 14 of the Compliance Requirements, records relating to the transition of training products are documented and retained. This includes transition plans, student communication, mapping

documents, and evidence of enrolment into replacement qualifications. These records are stored in the Transition Register and retained for audit purposes

H. USI Verification and Correction Procedure

KOIC verifies each student's Unique Student Identifier (USI) through its Student Management System (SMS) immediately after enrolment. The SMS communicates with the national USI Registry to confirm the accuracy of the data entered.

Staff must ensure that:

- The student's full legal name, as registered with the USI Registry, is entered without abbreviations (e.g., "Benjamin" rather than "Ben").
- The student's date of birth and USI are also entered exactly as recorded in their USI registration.

If the verification fails, staff are required to:

1. Cross-check the USI details with the student and confirm the correct spelling of their legal name.
2. Request an official ID or re-confirmation of the details used by the student when registering.
3. Update the student's record in the SMS and reattempt the verification.

If KOIC assists a student to create their USI, identity documentation (e.g., driver's licence, Medicare card) will be temporarily stored via the integrated Document Verification Service (DVS). These records are automatically deleted after USI creation, as required under the Student Identifiers Act 2014.

All USI data is stored securely, and access is restricted to authorised staff only. Verification logs and records of correspondence with the student are retained in accordance with the RTO's Records Retention Schedule.

I. Student Access to Records

KOIC is committed to ensuring students have timely and equitable access to their personal and academic records in accordance with the Privacy Act 1988 (Cth), the Standards for RTOs 2025, and, where applicable, Standard 10 of the National Code 2018.

Students may request access to:

- Enrolment records,
- Assessment outcomes and feedback,
- Attendance and participation records (where relevant),
- Support interventions,
- Completed student assessment evidence (for review, not alteration),
- Issued AQF certification documentation.

Request Process

1. Students must complete a Student Records Request Form, available from administration or online.
2. The request must clearly identify the type of record being requested and the reason for the request.
3. Students are required to present a valid form of identification (e.g., photo ID) before access is granted.
4. Access will be provided within ten (10) business days unless exceptional circumstances apply.

5. If a copy of records is requested (rather than viewing access), an administrative fee may apply. This fee is waived for students who only require access without printed copies.

Access Conditions

- Records may be viewed in the presence of a staff member to protect the integrity of physical documents.
- Electronic records may be printed or exported from the Student Management System and verified for accuracy before release.
- Under no circumstances will original documents be removed from the premises or edited by students.
- All access requests and outcomes are recorded in the Student Record Access Log for quality assurance purposes.

Correction of Personal Information

- If a student believes that the information held is incorrect, incomplete, or not up to date, they may request a correction by completing a Change of Personal Details Form. KOIC will investigate and update records accordingly, maintaining an audit trail of any amendments made.

Access and Regulator Requirements:

- Records must be available to ASQA or relevant bodies upon request.
- AVETMISS data is submitted as per NCVER timelines.
- Records will be retained in a format that ensures accessibility for the full retention period. Authorised personnel, auditors, and regulators will be granted access upon request in accordance with Clause 7 of the Compliance Requirements. Systems must support timely retrieval and secure transfer of records for audit, complaint handling, and legal verification purposes
- KOIC releases personal data to third parties only with the student's written consent, or where permitted by law.

J. Record Accuracy and Audit Assurance

To ensure the integrity, accuracy, and completeness of student records, KOIC conducts periodic integrity audits as part of its internal quality assurance system. These audits support compliance with the Standards for RTOs 2025, particularly in relation to assessment evidence, certification, data reporting, and student progression monitoring.

Audit Purpose:

The objective of the integrity audit is to verify that records retained in the Student Management System and archive storage:

- Accurately reflect student enrolment, progression, and assessment outcomes,
- Are consistent with AVETMISS and AQF data requirements,
- Meet the evidentiary expectations of the regulator,
- Can support the issuing of valid AQF certification.

Audit Scope and Method:

- Audits are conducted on a sample of at least 10% of all completions recorded in the previous quarter.
- Samples are selected randomly but proportionally across training products and assessors.
- Each sampled student file is reviewed for completeness using the Student Records Integrity Checklist, including:
 - Enrolment details (start/end dates, course code/title),

- USI verification and identification,
- Assessment outcomes and assessor feedback,
- Evidence of competency decisions (sufficiency, authenticity, detail),
- Credit transfer or RPL records (if applicable),
- Issuance of certification,
- Fees reconciliation and CoE accuracy (CRICOS only),
- PRISMS reporting (where applicable).

Audit Process:

1. The Compliance Officer plans the quarterly audit and selects the record sample.
2. A designated internal auditor or delegated team member reviews each file against the checklist.
3. Any anomalies, omissions, or inconsistencies are logged in the Audit Findings Register and presented at the next management review.
4. Corrective actions are implemented, and relevant staff are notified or retrained if systemic issues are identified.

Outcomes and Reporting:

- A summary of audit findings and improvement actions is recorded in the Continuous Improvement Register.
- If recordkeeping concerns relate to assessment practices, they are referred to the Validation and Assessment Quality Review process.
- Audits form part of the broader self-assurance framework and may inform internal audits, validation cycles, and external audit readiness.

K. Data Reporting Obligations

KOIC submits all mandated data sets to regulators on time, in the required format, and through the approved portals. Responsibility for each report is allocated to a single position to ensure clear accountability and continuity.

Reporting Line	Dataset / Purpose	Due Date / Frequency	Submission Portal	Responsible Officer
Total VET Activity (TVA)	Full AVETMISS-compliant enrolment, participation and outcome data for the previous calendar year	Last business day of February each year	NCVER AVETMISS File Upload (SMS export)	Compliance Officer
Quality Indicator Data	Learner Engagement & Employer Satisfaction survey results (RTO performance indicators)	30 June each year	ASQA Quality Indicator Online Submission Form	Compliance Officer
PRISMS notifications (CRICOS only)	CoE creation, enrolment variations, completions, course progress breaches, deferral/suspension/cancellation	Within 31 days of event (or 14 days for course-	PRISMS portal	Student Services Officer (SSO)

		progress breaches)		
USI transcript updates	Issuance of AQF certification (qualifications & statements of attainment)	Within 30 days of issuance	USI Transcript Update Web Service (via SMS)	Student Services Officer (SSO)
Annual Declaration on Compliance	CEO attestation that KOIC met the Standards for RTOs during the preceding year	31 March each year	ASQA online Annual Declaration form	Chief Executive Officer
State / funding-contract reports (if applicable)	Claims, commencements, completions, participation evidence	As specified in the contract schedule	State training authority portals (e.g., STS Online, SVTS)	Finance Officer

- Reporting deadlines are loaded into the **Compliance & Governance Calendar** with automated reminders 30 days and 7 days in advance.
- Data files are generated directly from the Student Management System (SMS) and validated with NCVER/ASQA validation tools before upload.
- A Data Submission Checklist must be signed by the responsible officer and counter-signed by the Compliance Officer (or CEO for the Annual Declaration).
- Evidence of each submission (validation report, portal confirmation receipt, copy of uploaded file) is saved in the Data Reporting Register for audit purposes.
- Any submission errors or resubmissions are logged as improvement actions in the Continuous Improvement Register.
- Relevant staff undertake annual refresher training covering AVETMISS specifications, PRISMS reporting rules, USI procedures and portal-specific updates.

L. Treatment of Records on Cessation of Operations

In accordance with the National Vocational Education and Training Regulator Act 2011, KOIC acknowledges its obligation to manage student records appropriately in the event of ceasing operations.

If KOIC is subject to closure, deregistration, or transfer of ownership, the following actions will be taken to safeguard student records:

Regulatory Transfer of Records

- Within 30 calendar days of ceasing to operate, the RTO must transfer electronic copies of student records to the Australian Skills Quality Authority (ASQA), or the relevant designated authority.
- This includes all records related to enrolment, progression, completion, and AQF certification for every student enrolled during the period of registration.

- Records must include:
 - Full legal name
 - Date of birth and USI
 - Residential postcode
 - Enrolment and completion dates
 - Qualification and unit codes and titles
 - Assessment outcomes
 - Certification issuance details
 - Fee records (where required under contract)

Format and Submission Requirements

- Records must be provided in an approved digital format (e.g., Excel spreadsheet or CSV export from the Student Management System), and in accordance with ASQA's prescribed reporting structure.
- All data is to be extracted from the SMS and checked for accuracy and completeness before submission.

Security and Continuity

- During transition, KOIC will ensure records are protected from alteration, unauthorised access, or loss.
- Hard-copy documents will be digitised where necessary and stored in a secure cloud or server location until transfer is complete.

Notification

- ASQA and any relevant funding or regulatory bodies will be notified formally, in writing, of the intention to cease operations and the availability of records for collection or upload.
- All actions will be documented in the Cessation of Operations Compliance Log and retained by the Compliance

Roles and Responsibilities

Role	Responsibility
CEO	Ensures organisational compliance with records and document management standards and legislative requirements; approves revised documents.
Compliance Officer	Maintains the Document Management Register, schedules reviews, and ensures secure storage and access. Conducts regular audits to ensure the integrity and security of student records. Ensure compliance with the <i>Privacy Act 1988</i> and other legislative requirements.
Student Services Officer (SSO)	Ensure student and operational records are accurate, securely stored, and accessible. Process and respond to student access requests. Ensure compliance with record retention and disposal requirements.
Directors of Studies ELICOS/VET	Oversee the accuracy and timeliness of academic records, including attendance and progress reporting. Ensure academic staff are trained in student record-keeping responsibilities. Monitor compliance with the <i>ESOS Act 2000</i> for ELICOS attendance and

	<i>Standards for RTOs 2015</i> for VET reporting. Liaise with academic staff to ensure accurate recording of results and assessment outcomes in the Student Management System (SMS).
Academic Staff	Maintain accurate student records and use only approved current versions of documents. Record student attendance, academic progress, and results in a timely manner. Provide accurate information to ensure up-to-date student records.

Policy Implementation

Implementation occurs through staff induction and ongoing training. Document control systems including the Document Management Register, file naming protocols, and review schedules are monitored by the Compliance Officer. Authorised access, cloud storage, and backup protocols are in place.

Monitoring and Review

Monitoring is conducted through scheduled audits, document review cycles, and self-assurance practices. Monitoring includes reviewing assessment validation records (Standard 1.5), student support interventions (Standard 2.2), and internal audit outcomes (Standard 4.3). The effectiveness of record and document controls is reviewed annually and post-incident. Continuous improvement actions are recorded and tracked.

KOIC's Records Management policy is reviewed every two years, or sooner as required, to reflect legislative changes and operational requirements.

Version Control

Version	Date	Description	Approved by	Approval date	Author	Review date
V1.0	Jun 2025	Consolidated Student Records Management Policy and Data Integrity and Provision of Information Policy in line with new standards for RTOs 2025.	CEO	20 June 2025	Compliance Officer	June 2027
V1.1	Apr 2026	Re-brand of policy to KOIC	CEO	1 Apr 2026	Compliance Officer	Apr 2028

Policy and Document Information

Author:	Compliance Officer
Policy owner:	Compliance Officer
Approved by:	CEO
Approved date:	1 Apr 2026
Status:	Approved
Next review due:	April 2028