Canberra Institute of Technology
RTO Code 0101 | CRICOS No. 00001K

Records Management Procedure

1. Associated Policy

The CIT Records Management Procedure has been developed in conjunction with the Records Management Policy.

2. Purpose

This document provides guidance for CIT staff on appropriate record keeping while ensuring compliance with the applicable Territory and Federal legislation and regulations.

3. Enabling Legislation and Guidance

3.1 This procedure is based on, and support, Federal or Territory legislation and guidance including:

- ACTPS Digital Records Policy
- Archives Act 1983
- CIT Records Management Program
- Copyright Act 1968
- Discrimination Act 1991
- Electronic Transactions Act 2001
- Evidence Act 2011
- Financial Management Act 1996
- Freedom of Information Act 2016
- Information Privacy Act 2014
- Public Sector Management Act 1994
- Territory Records Act 2002 (the Act)
- ACT Government Open Government initiatives

3.2 This document applies to all record management activities undertaken and managed by CIT.

4. Procedures

4.1 CIT are required to have a records management program that are supported by systems and processes that:

a) Support reliable recordkeeping;
b) Ensure recordkeeping is systematic;
c) Ensure recordkeeping is managed;
d) Allow recordkeeping to be audited; and
e) Make recordkeeping a routine part of transacting business.

4.2 Creation, Management and Control

4.2.1 CIT must ensure:

a) Full and accurate records of all CIT activities and decisions are systematically created by authorised people or systems to meet business needs, accountability requirements and community expectations.
b) Authentic records of all CIT activities and decisions are consistently captured by robust and compliant systems.

c) Public records are correctly and clearly associated to relevant times, people, systems, processes and events to ensure they are reliable evidence of what occurred.
d) Public records are preserved for future use at the time of their creation and capture through effective strategies, methods and formats.
e) Systems that capture public records maintain the integrity of the records as evidence, protecting them from undetected and unauthorised alteration.

4.1.2 CIT must ensure:

a) Metadata elements needed for the structure, context and management of business records to be used and understood over time are captured, maintained and connected with the records.
b) Business records are classified in accordance with business classification schemes that are aligned and mapped to access control and disposal programs.
c) Business records are accurately tracked using systems that create, capture and maintain information about the movement of and actions on records.

4.1.3 The value of a record is not dictated by its format, but by the:

a) Content (i.e. is it business related and whether
b) Scarcity (i.e. whether it is unique or one of many copies)
c) Context (i.e. the considerations that promoted its creation)

5. Staff Responsibility

Role	Responsibility
Chief Executive	• Provide support and resources for ensuring a successful Records Management Program. • Promote compliance with the CIT Record Management Policy and Procedures.
Executive	• Ensure that record keeping systems underpin and support business processes. • Appoint a Records Manager to manage day-to-day records management at CIT. • Ensure that the Records Management Program, Policy and Procedure are kept updated to reflect all record keeping requirements that CIT must meet. • Implement performance and evaluation measures to meet corporate objectives and relevant standards.
Records Manager	• Incorporate record keeping principles into business processes. • Arrange appropriate resources to enable the Records Management Program to be established and maintained. • Facilitate public access to records in cooperation with the CIT Freedom of Information officers and the ACT Government Reference Archivist. • Implement regular reviews and updates of the Records Management Program to ensure the entire Program is reviewed and updated at least every five years.

Records Management Staff	• Create and maintain record keeping procedures. • Promulgate record keeping procedures and practices to all staff. • Monitor staff compliance with the record keeping policy and procedures. • Provide record keeping training and advice to all staff. • Monitor and review the CIT record keeping system and tools. • Support consistent classification, titling, indexing and sentencing of records. • Ensure all digital records have appropriate access permissions. • Ensure that records are kept for only as long as the CIT and the public require them as established in approved functional Record Disposal Schedules.
Managers and Supervisors	• Monitor staff under their supervision, including consultants and contractors, to ensure that they understand and comply with record keeping policies and procedures. • Facilitate their staff in having access to tools, procedures, and expertise to assist them to carry out their record keeping responsibilities. • Ensure staff comply with their exit protocols in relation to records management. • Support and foster a culture that promotes good recordkeeping practices.

All staff	• Understand the record keeping obligations and responsibilities that relate to their position
	• Adhere to the policies and procedures and standards in their record keeping practice, for creating and capturing records of their daily work. This includes records for the following business activities:
	  ◦ Approval or authorization
	  ◦ Guidance given or direction
	  ◦ Information relating to projects or activities
	  ◦ Formal business communication to external bodies, students or other staff
	• Ensure that records are accurate, complete, meaningful, and adequate for the purpose for which they are kept.
	• Capture records in the appropriate CIT endorsed record keeping system in line with this procedure and the supporting local processes.
	• Manage physical records carefully to ensure their safe storage and good quality.

6. Record Keeping Systems

6.1 Hewlett Packard (HP) Content Manager (TRIM) is the primary, endorsed record keeping system at CIT for all records relating to the corporate business of the organisation.

6.2 Other endorsed systems are:

a) Physical files stored with the Records Management Unit
b) E-Learn (Moodle) for training and assessment records
c) Student Management System (Banner) for student enrolment records
d) CRM (Oracle) for student support records

6.3 The following are not endorsed for formal record keeping requirements:

a) Email accounts
b) Local network drives
c) Sharepoint
d) Microsoft Teams
e) Portable devices
f) Unapproved commercial systems
g) Personally owned computers
h) Any other location that could reasonably be considered as a risk to CIT record keeping.

6.4 Staff may store records temporarily in the non-endorsed systems outlined above, corporate records must be retained and managed on an appropriate file in the endorsed corporate system from the list in 6.2.

6.5 Document control measures must be put in place for all documents regardless of storage location, where those documents are used by multiple areas or managed via CIT-wide templates.

7. Digitisation

7.1 Digitisation of physical records is preferred by CIT however it is acknowledged that not all student assessment records can be digitised.

7.2 Every effort should be made to digitise all records or to retain the physical record in an appropriate storage facility with a record maintained of that storage to ensure appropriate retention and disposal activities.

7.3 The Records Management Unit will support digitisation of records, with a priority on student records.

8. Record Security

8.1 Records Protection and Security is concerned with the following:

a) **Confidentiality**: ensuring that information is accessible only to those authorised to have access.
b) **Integrity**: safeguarding the accuracy and completeness of information.
c) **Availability**: ensuring that authorised users have access to information when required.
d) **Responsible use**: ensuring that controls are in place so that users of IT systems are not able to adversely affect other users or other systems.
e) **Compliant Use**: meeting legal and contractual obligations.

8.2 The staff member who creates or receives the record from an external person or organisation is responsible for the assessment and application of the appropriate protection and security requirements.

8.3 Groups or types of records that may require alternate procedures include those whose unauthorised access, disclosure, loss of integrity, or unavailability may:

a) Seriously damage, or compromise, the success or adversely affect the viability, of a commercial venture or law enforcement process;
b) Cause distress to, or threaten, an individual (i.e. records containing personal information, e.g. HR personnel files, medical records, Aged or Youth records);
c) Have specific legislative restrictions or requirements;
d) Cause serious financial damage to and/or lead to litigation against the agency; and/or
e) Cause serious loss of public confidence.

9. Public Use and Access

All requests for records are processed in accordance with the appropriate act.

10. Performance Measurement

10.1 Record keeping performance measures managed by the Audit, Risk and Corporate Governance team include but are not limited to:

a) Audit of record keeping systems to ensure compliance
b) Assessment of any new and monitoring of current business information systems to ensure records are captured and managed appropriately
c) Annual file census to ensure accountability
d) Monitoring of functional thesaurus and record disposal schedules to ensure they are used appropriately
e) Quality control checks on all file creations/amendments/alterations to ensure consistency and in line with policy and procedures
f) Monitoring all record destruction activities to ensure consistency with record disposal schedules and in line with provisions of the Act
g) Obtaining feedback from staff on the quality and appropriateness of training
h) Monitoring or record keeping procedures to ensure practices are in line with the Records Management Program.