NMIT INFORMATION AND RECORDS MANAGEMENT PROCEDURE

MOKAMOKA WHAKAAETANGA | APPROVAL DETAILS

Section	Executive		
Approval Date	11.08.2026	**Sponsor**	Director Digital and Information
Next Review	01.01.2029	**Approved by**	SLT

NGĀ WHAKATIKATIKA | AMENDMENT HISTORY

Version	Effective Date	Created/ Reviewed by	Reason for review / comment
1	01.07.2026	Information and Records Management Advisor	New

Mō wai me te whānuitanga | Audience and scope

These Procedures apply to:

(a) All employees of NMIT, including contracted staff and secondees providing services for NMIT; and those on fixed term contracts (collectively referred to as kaimahi in these procedures).
(b) All business functions and activities of NMIT, including those performed by external contractors and consultants (references to kaimahi in these procedures include contractors and consultants unless otherwise specified).
(c) All physical and digital information and records, irrespective of format or medium, created, received and managed by NMIT kaimahi and related entities in the conduct of its business.
(d) All metadata associated with digital information, including data held in business systems and content information systems.

These Procedures exclude an individual's records or personal papers created in a private capacity, copies of documents used for reference, working papers and published research not covered by Intellectual Property legislation.

Te Pūtaki | Purpose

These Procedures give effect to the NMIT Information and Records Management Policy which should be read in conjunction with this document. It supports compliance with legislative requirements, including the Public Records Act 2005, and aligns with best practice standards for information management.

All principles stated in the Policy apply to these Procedures.

Tirohanga Whānui | Overview

Information and records are organisational assets and must be managed throughout their lifecycle, from creation and use through to retention and disposal, or permanent archive.

Ngā Haepapa | Responsibilities

Role	Responsibilities
Chief Executive Officer	Overall responsibility for ensuring NMIT meets its legislative obligations for information and records management.

Executive Sponsor (Chief Executive Officer)	Currently assigned to Chief Executive Officer • Strategic and executive responsibility for overseeing NMIT's information and records management practice. • Liaises with Archives New Zealand on monitoring and reporting of compliance
Senior Leadership Team and Managers	• Monitor and manage all information and records under their control and generated within their area of responsibility to ensure compliance with this Policy and all relevant legislation, including approving the disposal of records. • Support kaimahi by providing ready access to business rules and processes in their area of responsibility that meet record keeping requirements. • Embed relevant information management requirements into contracts with third parties.
Business System Owner	• Responsible for the procurement, operation, access, compliance and ongoing maintenance of a business system used within their area.
Information & Records Management Advisor	• Provide advice, training and support on information and records management best practice. • Develop the information and records management programme of works to support NMIT's strategic and operational information management requirements. • Initiate compliance auditing and communicate corrective actions.
Kaimahi	• Comply with this Policy, related procedures and business rules pertinent to their role. • Observe requirements for protecting information appropriately, particularly personal or confidential information.
ITCS and Digital Centre	• Provide, monitor and maintain approved business systems and tools to manage NMIT information and records, with appropriate mechanisms for managing accessibility, security, backup, disaster recovery and business continuity.

Ngā Hātepe | Procedure

1 INFORMATION AND RECORDS MANAGEMENT PROGRAMME

1.1 The Information and Records Management Advisor will maintain an ongoing programme of work to support compliance with legislative requirements and mandatory standards issued by Archives New Zealand. This includes:

- coordinating information management maturity assessments every five years, with annual progress reviews to monitor improvements and emerging risks;
- carrying out compliance reviews and communicating corrective actions to relevant kaimahi;
- providing information management training, guidance, and support to kaimahi; and
- coordinating improvement initiatives arising from audits, risk assessments, compliance activities, and organisational priorities.

2 RECORDS OWNERSHIP

2.1 Information and records created, received, or maintained by kaimahi in the course of conducting NMIT business are corporate records for which NMIT is responsible and must be managed in accordance with these procedures, associated policies, and applicable legislative requirements.

2.2 Business areas engaging third parties to provide services on behalf of NMIT must ensure contractual arrangements clearly define the ownership, management, access, retention, security, and disposal requirements for information and records associated with the service.

Prior to entering into contractual arrangements, the Senior Leadership Team (SLT) and Managers must ensure:

- ownership and custody arrangements are clearly defined;
- records remain accessible to NMIT during the retention period;
- legislative and regulatory obligations can be met;
- appropriate privacy, confidentiality, security, and disposal requirements are included; and
- records can be retrieved or transferred to NMIT in a usable format at the conclusion of the agreement, where required.

2.3 SLT and Managers must engage with the relevant business areas (e.g. ITCS, Legal Counsel, Information Management) where contracts, outsourced services, cloud systems, or third-party platforms involve the creation, storage, management, or disposal of NMIT information and records.

3 RECORDS CREATION AND CAPTURE

Electronic records

3.1 NMIT operates on a 'digital by default' basis wherever practicable, with records created, captured and maintained in digital format throughout its lifecycle.

3.2 Kaimahi must create, capture, maintain and manage full and accurate records of business activities, decisions, actions and transactions at the time the activity occurs, or as soon as practicable afterwards, ensuring records contain sufficient detail to provide reliable evidence of the activity or decision.

3.3 Kaimahi must save emails relating to business decisions or transactions within the relevant SharePoint folder or approved business system to support retention, disposal and business continuity requirements.

Naming electronic documents and folders

3.4 Kaimahi must ensure documents and folders are named clearly and consistently so they are easily identifiable and searchable within approved business systems. File names should be concise, meaningful, and only use recognised abbreviations where appropriate. Kaimahi should refer to File Naming Guidance for assistance.

3.5 Curriculum area kaimahi must use the approved SharePoint folder structure within their Programme Group workspace and save documents within the appropriate folders in accordance with the Programme Group Filing Index.

Physical records

3.6 Physical records must only be created or used where necessary for business, legal or operational purposes (e.g. ākonga assessment papers).

Share, reuse and discover

3.7 Information re-use is encouraged and unnecessary duplication should be avoided.

Kaimahi should collaborate on single documents where practical and refer to organisational single sources of truth rather than saving additional copies. Where multiple versions are required, version controls or approved naming conventions must clearly identify the current version.

SharePoint registers

3.8 Where SharePoint registers have been established for legislative or regulatory compliance purposes, kaimahi must save all related information and records within the relevant register. This includes:

- OIA Register
- Policy Register
- Procedures Register
- Privacy Register

4 STORAGE IN APPROVED SYSTEMS ONLY

4.1 Kaimahi must store business records within NMIT-approved business systems to support appropriate access control, audit capability, metadata capture, search and retrieval, retention and disposal management, and business continuity requirements.

4.2 Kaimahi must not store business records in personal drives, unauthorised cloud services, desktops or other non-approved systems.

4.3 Kaimahi are responsible for ensuring records within NMIT-approved systems remain organised and appropriately managed throughout their lifecycle.

5 RETENTION

5.1 Business records must be retained for the minimum retention period specified in the applicable Disposal Authority.

5.2 Kaimahi must refer to the relevant Disposal Authority to determine retention requirements or seek guidance from the Information and Records Management Advisor.

- GDA6 applies to records common across corporate organisations, including property, personnel, and financial management records.
- DA424 applies to records unique to tertiary education providers, including student administration, student services, teaching and learning, research, and the management of these areas.
- GDA7 applies to administrative and transitory records, including meeting invites, draft documents, and duplicate records.

5.3 NMIT will progressively implement automated retention and disposal functionality within SharePoint and other approved approved business systems to support compliant and efficient information lifecycle management.

6 DISPOSAL

6.1 Business records should only be destroyed once the applicable minimum retention period has expired and records are no longer required for business or legal purposes. Records containing personal information should be destroyed as soon as the minimum retention period has expired. Destruction should occur in accordance with the requirements set out below.

6.2 Prior to disposal, kaimahi must consult the relevant Disposal Authority and ensure:

(a) the retention period has expired;
(b) the Disposal Action is *Destroy*; and

(c) the records are not subject to an Official Information Act request, investigation, audit, or other business requirement.

6.3 For physical records approved for destruction, kaimahi must:

(a) complete the Request for Approval to Destroy Records form;
(b) obtain manager approval prior to destruction;
(c) save the approved form in the *Disposal of Records* folder with the SharePoint Compliance folder for audit purposes; and
(d) place the records into a blue secure destruction bin.
(e) Contact Campus Services when the blue secure bin is full so they can arrange a replacement bin.

6.4 Records covered by GDA7 do not require evidence of destruction. However, physical records containing sensitive or personal information must be destroyed using the blue secure bins.

6.5 For digital records approved for destruction, and until automated retention and disposal functionality is implemented within SharePoint, kaimahi must move records into the approved Archive Folder within SharePoint or seek guidance from the Information and Records Management Advisor.

6.6 The Information and Records Management Advisor will coordinate the annual destruction of eligible physical records held within Archive Store following approval from the relevant manager.

6.7 Any kaimahi who become aware of the unauthorised disposal of a business record must notify the Information and Records Management Advisor as soon as practicable. Unauthorised disposal also includes the accidental loss or damage of a business record. The Information and Records Management Advisor will record the incident in the Unauthorised Disposal Register and take any necessary follow-up action.

7 ARCHIVE

7.1 Kaimahi are responsible for ensuring NMIT records identified for permanent retention under the relevant Disposal Authority are retained within approved business systems or, where held in physical format, retained in NMIT's Archive Store, prior to being transferred to Archives New Zealand.

7.2 Where physical records are identified for permanent retention, kaimahi must:

- complete a Transfer to Archive Store Request form;
- box and index the records in accordance with Archive Store requirements; and
- email records@nmit.ac.nz to arrange transfer to Archive Store.

7.3 Archive Store is a restricted-access area. Kaimahi requiring access must contact the Information and Records Management Advisor to arrange entry. Kaimahi accessing Archive Store must sign in and out using the designated access register. Any archival records removed from Archive Store must be recorded in the Archive Register, including the date removed and expected return date. The Archive Register must be updated upon return of the records.

7.4 Where business areas are considering digitising original paper records, they must first determine whether the digitised copy is intended to replace the original paper record or be created as a use-copy while retaining the original. They must also assess whether the records have historical, cultural, legal, or evidential value requiring retention in the original format. Guidance must be sought from the Information and Records Management Advisor before digitising original paper records where there is likelihood the records meet these criteria. Where a digitised record is intended to replace the original, the digital record must be complete, accessible, and stored in an approved business system before the original paper record is destroyed.

7.5 Where digital records are identified for permanent retention, and until automated retention and disposal functionality is implemented within SharePoint, kaimahi must move records into the relevant Archive folder within SharePoint or seek guidance from the Information and Records Management Advisor.

7.5 Transfer of custody of NMIT records to Archives New Zealand will be coordinated and documented by the Information and Records Management Advisor in consultation with the relevant manager, including determining applicable open access periods prior to transfer.

8 LIFECYCLE AND SYSTEMS

Lifecycle management

8.1 Kaimahi must manage information and records throughout their lifecycle from creation or receipt through to authorised disposal or archival preservation.

To support this, kaimahi must:

- store electronic records in accordance with section 3 of this Procedure
- store physical records, including kaimahi and ākonga files, in secure locations with access limited to authorised kaimahi, and
- ensure records remain accessible, useable, and discoverable for the duration of their retention period.

Approved business systems

8.2 To support compliance with Archives New Zealand Information and Records Management Standard, business and curriculum areas must consider information and records management requirements during:

- procurement;
- system development;
- system upgrades;
- migration projects; and
- system decommissioning activities.

Business system owners are responsible for ensuring approved business systems support the ongoing accessibility, integrity, authenticity, usability, and discoverability of records. When implementing system changes or carrying out migration activities, business system owners must ensure records, metadata, and contextual information remain preserved, accessible, reliable, and usable throughout the process.

8.3 Business systems owners must engage with the Information and Records Management Advisor early when planning system changes to ensure records are appropriately retained, migrated, archived, or disposed of.

Digital continuity

8.4 The Information and Records Management Advisor will periodically assess long-term digital information to ensure it remains reliable, accessible, and usable, and will coordinate remedial action where risks to digital continuity are identified.

8.5 ITCS and the Digital Centre are responsible for monitoring and maintaining approved business systems, applications, and tools that manage organisational information and records, including implementing controls for system access, security, backup, disaster recovery, and business continuity.

8.6 Business continuity and disaster recovery arrangements must support the protection, recovery, and continued accessibility of high-value information and records.

9 OFFICIAL INFORMATION ACT COMPLIANCE

9.1 Kaimahi must manage information and records in a manner that supports timely responses to requests made under the Official Information Act.

9.2 Kaimahi must not improperly delete, alter, conceal, or remove records that may be required for Official Information Act requests, privacy requests, audits, investigations, legal proceedings, or business continuity purposes.

10 SECURITY, PRIVACY AND PROTECTION OF INFORMATION

10.1 Kaimahi are responsible for protecting the information and records they create, access, use and share, and must ensure information is only accessed, used or shared for authorised business purposes and in accordance with its sensitivity and risk.

10.2 Documentation shared externally must only be shared through approved business systems. Where external parties require access to SharePoint folders or documents, or assistance is required with external sharing, kaimahi must complete the External Guest Access form to ensure appropriate permissions and time-limited access are established.

10.3 ITCS is responsible for periodically reviewing external guest access accounts and disabling access once it is no longer required.

10.4 Kaimahi must not use SharePoint ‘share links’ to provide documentation to ākonga. This restriction is in place to protect personal information, maintain appropriate access controls, and prevent unintended access to organisational content. Where documents stored in SharePoint need to be shared with ākonga, they must first be downloaded and then provided as an email attachment or via an approved external sharing method.

10.5 Kaimahi must not create, store, sync, forward, or share business records through personal or unauthorised email accounts, devices, storage locations or sharing platforms unless prior approval is granted by ITCS or the Digital Centre.

10.6 Notwithstanding the above, kaimahi and ākonga records, or other highly sensitive or personal information, must **never** be stored in non-approved business systems.

10.7 Prior to the transfer of records to Archives New Zealand, the relevant Manager in consultation with the Information and Records Management Advisor, must determine the records' access status (open or restricted). Where records are classified as restricted, the Manager must document the reason for the restriction (e.g. personal privacy, commercial sensitivity or legal privilege) and the restriction period, in accordance with the Public Records Act 2005 and Archives New Zealand requirements.

11 LEGISLATIVE FRAMEWORK

11.1 Kaimahi will manage their information and records in accordance with applicable legislative and regulatory obligations.

11.2 The Information and Records Management Advisor will carry out monitoring and audit activities across physical and digital information environments to support compliance and continuous improvement.

11.3 Non-compliance will be reported quarterly to the Director of Digital and Information with corrective actions communicated to relevant kaimahi.

Ngā Tikanga | Definitions

Term	Definition
Archives New Zealand	Department of Internal Affairs division that administers the Public Records Act
Business rule	Rules established by NMIT to ensure that business needs are met, and consistent records management practice is implemented, particularly for processes not governed by Archives New Zealand approved disposal authorities.
Business systems	IT systems that create, capture, store, manage and provide access to electronic data, information and records. Includes either line-of-business systems and content information systems. Excludes personally owned devices and non-NMIT storage/databases.
Creation and maintenance	The process and act of creating records that are accurate, authoritative, and reliable; and managing these records over time in a way that ensures their accessibility and usability for as long as it is necessary to meet legal obligations and business requirements.
Data	A general term meaning facts, numbers, letters, and symbols collected by various means and processed to produce information.
Disposal	Disposal is the process of eliminating, deleting or destroying a record or records, beyond any possible reconstruction. For paper records that means using secure destruction bins; for electronic records it means permanent deletion i.e. the information is not retrievable.
Disposal Authority DA424 ITPNZ	Formal authority granted to NMIT by the (Archives New Zealand) Chief Archivist setting out the authority and criteria for retention and disposal of records specific to Institutes of Technology and Polytechnics.
Electronic record	Any record that is created or stored by digital means including documents, databases and emails.
Executive Sponsor	Person within an organisation who is assigned strategic and managerial responsibility for the oversight of information and records management.
General Disposal Authority (GDA6)	Formal authority granted to NMIT by the (Archives New Zealand) Chief Archivist setting out the authority and criteria for retention and disposal of specified records not listed in the sector-specific authority. It includes HR, finance, and other common corporate records.
General Disposal Authority (GDA7)	Formal authority granted to NMIT by the (Archives New Zealand) Chief Archivist setting out the authority and criteria to dispose of routine records that do not form part of NMIT's core business records and have only temporary, administrative or reference value.
Information and records management	Oversees the lifecycle of information, from creation to disposal, including the process for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records (also referred to as record keeping).
Information	Information is data that has been processed, organised, or structured to provide meaning, context and usefulness. Information forms the basis for records and includes content in various formats that support decision-making or business activities – including documents, email, data, images, digital files and on any medium (e.g., paper, film, tape, CD or electronic systems and devices).
Metadata	Structured information that describes, manages, controls, and preserves information through time. This can include the file name, date range, unique identifier or document properties.
Migration	The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability.
Records	Information created, received, and maintained by NMIT as evidence of its business activities, transactions, or legal obligations. Records support organisational functions and may exist in any format and on any medium (see *Information* above).

Ngā Hononga ki Tuhinga kē | Links to other documents

NGĀ KAUPAPA-HERE E HANGAI ANA | RELATED POLICIES

NMIT Information and Records Management Policy
NMIT Official Information Act Policy
NMIT Privacy Act Policy
NMIT ICT Security Policy
NMIT Business Continuity Management Policy

NGĀ TUKANGA ME NGĀ HĀTEPE | RELATED PROCESSES, PROCEDURES

NMIT Official Information Act Procedure
NMIT Privacy Act Procedure
NMIT Data Breach Response Plan
NMIT Business Continuity Plan

TURE WHAI TAKE | RELEVANT LEGISLATION

Education and Training Act 2020
Public Records Act 2005
TEC Recordkeeping Requirements when receiving TEC funding
NZQA Quality Assurance of Education Providers Rules 2026

NGĀ TAPIRITANGA | APPENDICES