Controlled Document – Refer to NMIT website or intranet for latest version

NMIT ICT SECURITY POLICY

MOKAMOKA WHAKAAETANGA | APPROVAL DETAILS

Section	Executive		
Approval Date	24.02.2026	**Sponsor**	Director Digital, Finance and Risk
Next Review	01.01.2027	**Approved by**	SLT

NGĀ WHAKATIKATIKA | AMENDMENT HISTORY

Version	Effective Date	Created/ Reviewed by	Reason for review / comment
1	01.01.2026	Transition Lead	New

Mō wai me te whānuitanga | Audience and scope

This policy applies to:

a) All employees of NMIT, including contracted staff and secondees providing services for NMIT; and those on fixed term employment contracts (may be collectively referred to as kaimahi in this policy); and
b) Contractors and other parties external to NMIT who access or use NMIT services and/or infrastructure on a temporary basis to support NMIT and would not normally be considered kaimahi (but are included in reference to 'users'); and
c) All governors of NMIT including members of NMIT Council and governance committees or boards (collectively referred to as governors in this policy); and
d) All ākonga of NMIT engaged in campus-based learning at any location; and online or remote learning via any mode; and work based learning. This includes (eg.) managed apprentices, Trades Academy and other secondary-tertiary pathway learners, and any other non-standard enrolments, and encompasses all references to learners, ākonga or students.

Te Pūtaki | Purpose

NMIT is committed to ensuring its information and communication technology (ICT) assets are protected and secure, that information security risks are known and mitigated, and that our practice is legally compliant.

The purpose of this policy is to provide clear guidance about:

- our collective responsibilities and obligations to ensure the security of NMIT's ICT and data, and the protection of NMIT's business information systems and IT network from misuse and damage
- what constitutes acceptable and unacceptable use of NMIT's IT services, systems and infrastructure

It covers all ICT hardware and software, data, services, systems and associated infrastructure and devices that are owned, controlled or operated by NMIT, and/or are connected to the NMIT IT network.

Data refers to all information and records, including any form of electronic message sent or received internally or externally (including any attachments) created or maintained in the course of NMIT's business on any device.

Ngā Mātāpono | Principles

Maintaining the safety and security of NMIT's ICT and data is a collective accountability, and a requirement for all users of NMIT ICT systems and services.

NMIT invests in, advocates and enables the use of ICT hardware, services and systems to ensure:

Compliance
Decision-making and practice will comply with all relevant legislation, standards, policies and procedures, and any agreements binding NMIT to implement applicable security safeguards.

Risk Management
NMIT is protected against unauthorised access to, or unauthorised use or sharing of data which could potentially result in harm to NMIT, members of the NMIT community, or NMIT operations

Information security assurance is enabled through clear lines of responsibility and controlled access to NMIT platforms, data and information.

Service Quality
NMIT's decision-making and management will enable and support reliable, efficient, consistent practice that meets the needs of the institute and its operations.

Best Practice
NMIT will implement practices that support and develop resilience, good practice and accountability in planning for, managing and responding to ICT security needs.

Kaupapa Here | Policy Statements

ICT User Obligations

NMIT computer devices, services and systems are provided to enable kaimahi with their work, and to support ākonga during their learning journey once they are fully enrolled.

Devices, services and systems may be made available to guests, contractors or other external parties as required.

Kaimahi are required to use an NMIT-provided or endorsed system or service in their day-to-day work if a suitable system is available for that purpose.

All users of NMIT's ICT systems, services and devices will

- use them for their intended purpose, ie. teaching, learning, research, communication, support and administration of these activities
- use systems and services in a manner that does not expose NMIT to security or commercial risk; or compromise the confidentiality of NMIT data; or degrade or impact other users of those systems
- comply with all legislative requirements, policy and procedures that apply to the use of NMIT ICT systems and services, and to the legal and ethical creation, collection, storage, use, retention and disposal of NMIT data and records.

Misuse of NMIT information, communication and technology assets, whether intentional or negligent, is a breach of this policy and will be pursued in accordance with the relevant investigation and disciplinary policies and procedures.

NMIT reserves the right to block or limit access to the internet and services that are not considered acceptable for that user's role.

Objectionable or Inappropriate Material

Sites classified as criminal or undesirable, as adopted by NMIT under subscription to an external service, are blocked. Visits to any website, including attempted visits to blocked sites, are recorded down to individual user level.

Accessing or using offensive, obscene, discriminatory, pornographic or otherwise inappropriate material through the internet or on the computer system is not permitted.

A user's access may be withdrawn if that user is found to be knowingly accessing, receiving, possessing or sending objectionable or inappropriate material using the NMIT computer systems.

Inappropriate use of the computer systems can result in disciplinary action.

File Storage and Ownership

Regardless of the ownership of devices used while conducting NMIT business, all information and records created in or uploaded to these devices in the normal course of NMIT business are the property of NMIT.

Electronic files and data used in the line of NMIT business **must only** be stored in NMIT-approved file stores.

NMIT data or software must not be stored or passed on to a non-approved file store or non-NMIT approved user.

In exceptional circumstances, kaimahi may temporarily need to use a non-approved NMIT file store for non-sensitive purposes. In such cases, a non-approved file store may **never** be used for storing the following types of records:

- Employee records, including information/data that can be used to identify specific employees
- Student records, including any information/data that can be used to identify individual students
- Files containing highly sensitive or confidential data

NMIT acknowledges it ethical and legal obligation to protect personal information that is collected and stored in the course of its business activities.

Access to NMIT Systems Off-Campus

When accessing NMIT systems off campus, kaimahi and ākonga are responsible for security of information, maintaining user vigilance, and adhering to all applicable NMIT policies and procedures.

Restricted Access to NMIT Business Information Systems

Access to information contained in specific restricted business information systems is subject to additional security protocols, due to the personal and potentially confidential nature of the information.

Software Installation and Licensing

The installation of all software or applications on an NMIT-provided or endorsed device requires the approval of the NMIT Digital team. The Digital team is responsible for ensuring that any software or other application, including cloud-based solutions, fit within the various NMIT requirements and avoid potential duplication or performance, operational or legal issues.

For clarity, on a user-owned device that has been endorsed by the Digital team for NMIT use, the NMIT Digital team approval is required for applications that are installed on that device specifically for NMIT business purposes.

Mobile Devices – Phones and Laptops

Kaimahi are responsible for the security and compliant use of any mobile device used to carry out NMIT business, irrespective of whether the device is NMIT-owned or privately owned, as specified in **NMIT ICT Security Procedures**.

Email, Text and other Electronic Messaging

Any email, text or other electronic message or recording that relates to any aspect of NMIT business is subject to this policy, the **NMIT Information and Records Management Policy** and all other relevant policies and/or procedures.

Forwarding NMIT business-related email or message to a personal or unprotected platform is not permitted.

Password Management

Passwords are a key security measure. All kaimahi are accountable for the creation, confidentiality, security and use of passwords where required to access NMIT systems and accounts.

Personal Use

Reasonable personal use of NMIT ICT is permitted. NMIT does not permit its ICT network to be used for personal financial gain or for private business purposes.

NMIT accepts no liability or responsibility for any personal use of its IT network or for loss of any personal content in an NMIT-approved file store

Training

All users will engage in relevant training designed to keep them up to date in the appropriate use of ICT systems and raise awareness of dangers and risks to the NMIT network and data when using ICT systems.

Security and Breaches

Users of NMIT systems and electronic services will adhere to NMIT's ICT security requirements at all times and will report any breach or suspected breach of security or privacy to the ICTS team immediately.

Monitoring

At any time and without prior notice, NMIT reserves the right to monitor, access, inspect or lawfully disclose any information stored on or transmitted through its information systems to ensure compliance with NMIT's policy and legal obligations.

Ngā Haepapa | Responsibilities

Role	Responsibilities
Digital teams – ITCS, Digital	Approval, allocation and management of all NMIT devices, services, software and systems to kaimahi, guests and other authorised users. This includes endorsement of non-NMIT supplied devices. Provide user training to raise awareness, support good practice, and minimise risk to NMIT.
Information and Records Management Advisor	Support and ensure users' adherence to **NMIT Information Management Policy** to ensure NMIT complies with all legislation and ethical requirements relating to information storage.
ICT Users	Maintain the safety and security of NMIT's ICT and data. Ensure that NMIT's intellectual, data and physical assets are protected by adhering to stated computer security practices. Hold personal accountability for the security of activities and files under their NMIT account.

Ngā Tikanga | Definitions

Term	Definition
Account	Login assigned to an individual user permitting access to carious systems.
Business Information system	Any database storing information as a structured record e.g. Student Management System
Data	All information and records, including any form of electronic message sent or received internally or externally (including any attachments) created or maintained in the course of NMIT's business on any device.
ICT	Information and Communications Technology
Mobile device	For the purposes of this policy, mobile device refers to: • A mobile phone, Smartphone, or similar highly portable device operating primarily on the mobile phone network; or • A portable laptop, tablet or combination unit thereof
Objectionable material	Includes all material which is objectionable as defined in the *Films, Videos and Publications Classification Act 1993*, and any material which could reasonably be described as unsuitable or offensive having regard to the circumstances in which, and the persons to whom, it becomes or may become available.

Ngā Hononga ki Tuhinga kē | Links to other documents

NGĀ KAUPAPA-HERE E HANGAI ANA | RELATED POLICIES

NMIT Kaimahi and HR Policy
NMIT Kaimahi Code of Conduct
NMIT Privacy Policy
NMIT Information and Records Management Policy
NMIT Student Charter and Student Rules

NGĀ TUKANGA ME NGĀ HĀTEPE | RELATED PROCESSES, PROCEDURES

NMIT ICT Security Procedure

TURE WHAI TAKE | RELEVANT LEGISLATION

Films, Videos, and Publications Classification Act 1993
Privacy Act 2020
Official Information Act 1982
Public Records Act 2005