Nelson Marlborough Institute of Technology
Te Whare Wānanga o Te Tau Ihu o Te Waka a Maui

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

IT ACCEPTABLE USE POLICY

Section	People and Organisation Development		
Approval Date	22.08.2017	**Approved by**	Executive Team
Next Review	29.11.2022	**Responsibility**	Executive Director – Strategy, Enterprise and Sustainability
Last Review	29.11.2019	**Key Evaluation Question**	6

PURPOSE

To define acceptable use of NMIT's IT services and infrastructure by employees and access account holders (referred to collectively in this policy as 'users').

To ensure that the Institute's Business Information Systems and IT network is protected from misuse and damage.

To clarify responsibilities and reduce potential liability for the Institute and all users in using all NMIT's IT services.

To protect personal information that NMIT collects and stores in the course of its business activities including learning and teaching.

SCOPE

Any person permitted to access, attempt to access or make use of NMIT's IT network and associated systems. This includes all employees, Contract for Service (CFS) individuals, contractors, sub-contractors, partners/joint ventures, consultants and visitors to NMIT.

All information and communications technology hardware and software, data and associated infrastructure and devices that are owned, controlled or operated by NMIT, and/or are connected to the NMIT IT network. These may include, but are not limited to: computers (including desktops and mobile devices), computer systems, USB sticks, CDs, DVDs, memory cards, external hard drives, cameras, (such as video, digital, webcams), video and audio players/receivers and telecommunication equipment, networks, software, cloud services, databases and any similar technologies as they come into use.

All material, including any form of electronic message sent or received internally or externally (including any attachments) created in the course of NMIT's business activities on any device.

DEFINITIONS

The ***NMIT Academic Statute - Section 2: Definitions*** lists the academic terminology used throughout this Policy. The definitions of specialist terms relevant to this Policy are listed below.

Account	Login assigned to an individual user permitting access to various systems.
Business Information System	Any database storing information as a structured record e.g. Student Management System
CFS	Contract for Service. An individual who is not an NMIT employee but who provides a service to the institute based on a business need.
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 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.
System Administrator	NMIT Staff member with delegated responsibility for system control.
User	Any individual having authorized access to the NMIT IT network or computer systems, whether internally or externally.
VPN	Virtual Private Network providing secure remote access to NMIT IT systems. Used only by 'high privilege' administrators, normal users go via web portals.

RESPONSIBILITIES

All users are responsible for ensuring that the intellectual, data and physical assets of the Institute are protected by adopting accepted computer security practices.

All users are personally accountable for the security of activities and files under their NMIT account, and must not share their log in with anyone.

Managers are responsible for approving appropriate access to IT services and ensuring that training needs for NMIT employees and CFS individuals in the use of NMIT computer systems are identified and provided.

POLICY

NMIT computer devices, services and systems are provided to assist users with their work.

Records, including electronic data, files and documents created in the normal course of NMIT business are the property of NMIT.

NMIT will not accept liability arising from personal use of the Institute's IT Network. The Institute's IT network may not be used for personal financial gain or for private business purposes.

Reasonable personal use of the internet and work email is permitted, but should be kept to a minimum and should not interfere with work responsibilities, encroach on working hours, or adversely affect systems performance.

Users must comply with the terms of any licence agreement between NMIT and any third party that governs the use of software or online resources.

Sites classified* as criminal or undesirable 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.

** The classifications are adopted by NMIT by subscription to an external service.*

SECURITY

All users must:

- Select a 'strong' (difficult to guess using specific criteria) password or passphrase, keep it secure, and not let any other individual operate under their account login. All users are responsible for all activity under their own account.
- Immediately report any known or suspected security breach, unauthorised access to confidential information, including the loss of any mobile devices containing NMIT data, or divulging of account credentials, to the IT Service Desk.
- Not knowingly introduce a virus or malware to the NMIT network or circulate one.
- Be aware and stay updated on what constitutes suspicious emails, attachments, website links etc. and always exercise caution interacting with such.
- Ensure that the Institute computer security processes are supported and not overridden or ignored.
- Not do anything to unnecessarily delay the application of security patches.
- Only connect devices authorised by Information Technology Customer Services, (ITCS), to the NMIT network and ensure that hardware or software is not modified, added or removed without their prior authorisation.
- Ensure that they do not disclose any personal information about other employees or students without consulting the NMIT Privacy Officer (The Privacy Officer for NMIT is the Chief Executive). No personally identifiable information pertaining to a student should be shown to them on screen without a) ***first*** verifying their identity and b) ensuring only their information is being shown.
- Ensure any personal devices or NMIT-owned devices that are connected to the NMIT computer systems have appropriate security protection.
- Ensure access to data is kept secure by always correctly exiting their sessions as soon as finished, and always locking their device before leaving it unattended for any length of time.

EMAIL

Users must exercise discretion in the content as email messages may be accessed by users other than the intended recipients.

Email messages sent or received using the Institute's facilities are the Institute's property. NMIT reserves the right to monitor, access and to disclose email messages.

Email messages are business records and must be appropriately worded. Where email messages record business decisions or document a part of the business process these messages should not be deleted in order to meet records retention and disposal criteria.

Forwarding of NMIT business related email to personal email accounts is not permitted, as they are not protected from unauthorised access.

TEXT MESSAGING

Text messaging from the Student Management System is limited to short, one-way texts to individuals or course groups who have consented to receive texts.

Text messaging to and from NMIT authorised mobile devices must be primarily business related, with use of personal messages kept to a reasonable amount.

EMPLOYEE/CONTRACTOR/CFS ACCOUNTS

Once a contract has been signed, and entered onto the HRIS system by People and Organisation Development team, users should have an individual computer network account generated automatically within 24 hours. This account automatically provides access to the following services:

- Staff ID card
- Any networked PC
- Wireless network
- Internet
- Polly Intranet
- Email and Office 365 account
- Individual and shared file stores
- Polly Staff Portal (off campus services)

Users must change their default password at first login and then are forced to by the system every 3 months thereafter. Passwords must adhere to the 'strong' protocol (enforced by the system).

On termination of a contract within the HR system, the account is automatically expired (closed but not deleted) within 24 hours, usually overnight. The account is kept closed for one year, with access available to the Line Manager on request, after which it, and all of its contents, are completely deleted.

TEMPORARY/GENERIC ACCOUNTS AND VISITOR / 3RD PARTY ACCESS

The creation of temporary/generic accounts is only permitted where an existing staff or student account is inappropriate, such as for exams or external hire, and must be assigned to a responsible NMIT owner/manager. Every account must have a named owner recorded, along with an automated account expiry enforced, not exceeding one year.

NMIT provides a Guest Wi-Fi service for on campus visitors wishing to connect non-NMIT owned devices to the internet. Connection will be granted for the duration of the specific event or task requiring such access, and subject to provisions in this policy. Access is not transferable to other individuals.

CFS and 3rd Party personnel accessing all other NMIT systems must request a personal account above via IT ServiceDesk backed by an approved NMIT staff sponsor, and sign a confidentiality form to protect NMIT data.

ACCESS TO SYSTEMS OFF-CAMPUS

When accessing NMIT systems off campus, (e.g. from home on any personal device), security of information and user vigilance must be maintained (e.g. lock computer when unattended, protecting device with a password/passcode at all times).

Most systems are accessible off-campus via secure web services i.e. the Polly Staff Portal on the NMIT website.

VPN/remote access to certain services on the main network will only be granted after confidentiality forms have been signed by nominated individuals for the following circumstances:

- System Administrators whose system is not available via the Staff Portal
- Users working primarily offsite whose system is not available via the Staff Portal
- 3rd party technical departments supporting core systems

FILE STORAGE

Electronic files and data used in the line of NMIT business must only be stored in NMIT-approved file stores. Any personal content in such should be kept to a minimum, and NMIT has no liability for loss.

NMIT-approved file stores include:
Network shared drives, (G: & L: drives)
Polly Intranet
NMIT Office 365/SharePoint/OneDrive
NMIT-owned mobile devices
Corporate databases and information systems

Non-approved file stores include:
Local NMIT computer drives (C: & D: drives)
Portable storage devices such as USBs, memory sticks, external hard drives
Privately owned computers and mobile devices
Cloud file stores accessed via an individual's own non NMIT account
Any other external stores not approved by ITCS

Non-approved file stores are deemed insecure due to limited or unknown ability to restrict access to authorised NMIT account holders only. Therefore no NMIT line of business content should be saved to them. This includes copying or syncing of data from NMIT-approved stores.

Despite the fact all NMIT-approved stores are easily accessible on or off campus, in some circumstances, e.g. approved Bring Your Own Device arrangements, NMIT staff may temporarily need to use non-approved NMIT file stores, but should **never** store the following types of records on such:

- 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

Regardless of the ownership of the devices, any records, messages, files and documents created in the normal course of NMIT business created in or uploaded to these devices are the property of NMIT. Users must adhere to this Policy when managing the devices and the NMIT business information they hold.

NMIT data or software must not be passed on to a non-approved NMIT file store or non-NMIT approved user, except in approved cases e.g. external technical support personnel.

SOFTWARE INSTALLATION & LICENSING

Whether a user has the ability or not to install software on a device, the licensing and approval remains the responsibility of ITCS. Users should always check the validity of software installs with ITCS *prior*, in order to avoid potential duplication, performance, operation or legal issues.

If software is for the use of more than one individual, whether 'on premise' or cloud based, ITCS must be consulted at the earliest possible stage to ensure a good fit for all NMIT requirements and platforms.

MOBILE DEVICES [MOBILE PHONES AND LAPTOPS]

The following covers **additional** and **unique** policies relating to **mobile devices,** categorised as follows**:**

Privately owned but containing NMIT content

- The device must have a PIN and/or passcode operational at all times. It is the responsibility of the user to ensure this is enabled.

NMIT-owned mobile devices

GENERAL USAGE

- Mobile devices should always be with the owner during work hours.
- The NMIT-issued device and **all** its contents remain the property of NMIT.
- Usage is monitored and needs to comply with all aspects of this policy
- Users are not to make or receive business calls on a mobile phone of any kind while operating a vehicle, unless an approved hands free device is fitted

SECURITY & CONTENT

- The user to whom the mobile device has been assigned is responsible for its safekeeping and for all activity with it.
- The device must have a PIN and/or passcode operational at all times. It is the responsibility of the user to ensure this is enabled.
- The device is solely for use by contractors for services of NMIT.
- Personally acquired apps may be installed providing they do not compromise the functioning of the device.
- NMIT reserves the right to directly and indirectly manage the device at any time, including remote wiping where necessary.
- Where the system update process is not fully automated, the user is responsible for timely actionning of prompts to apply updates.
- Lost, broken or malfunctioning units should be reported to ITCS immediately. Departments or end users may be required to contribute to replacement costs where caused by excessive negligence.
- Factory reset (full wipe) can often be the solution to resolving problems. NMIT has no liability for any personal content or apps lost that were stored on the device, nor any responsibility to recover such.

SUPPORT & TRAINING

- ITCS will only provide training and support on approved NMIT applications e.g. Office 365, Skype for Business. All other app installations are considered personal.
- Personal apps, especially free ones, may cause performance issues or incur unforeseen costs. Users should research possible impacts before installing. ITCS does not support any issues arising from such, and may return the device to base image if considered to be adversely impacting on its functioning.

- Users must make themselves available for training on the mobile device when advertised.

COST MANAGEMENT MOBILE PHONES

Usage costs are monitored and if they frequently or significantly exceed the normal contractual average and are attributable to non-NMIT activity, costs may be recovered from the individual.

Whilst all phones come with a monthly quota of data, calls, texts etc, users should always have the default setting as 'connect to free Wi-Fi' rather than mobile data networks wherever possible.

The owner has responsibility for recognising when they are incurring costs i.e. knowing when on mobile data or Wi-Fi networks, using mobile data within or over contract limits.

For international travel, mobile data roaming should be turned off, (use free Wi-Fi wherever possible). Data packs should be obtained for specific countries beforehand, (7 days notice). When overseas, personal calls should be kept to a minimum.

Whilst mobile phones are provided to assist team members in fulfilling NMIT business, NMIT recognises that team members may need to use the phone for personal use from time to time. Reasonable use for personal communication is allowed as long as it does not interfere with the team member's performance. Devices are never to be used for individual "business" or private matters relating to income-generating activities.

REFERENCES

INTERNAL

Copyright
Employee Involvement in Consulting and Outside Business Activities
Harassment (Prevention and Management)
Records Management Policy
Staff Misconduct Procedure
Staff Social Media policy

EXTERNAL

Privacy Act, 1993
Public Records Act 2005
Human Rights Act, 1993
Harassment Act 1997
Films, Videos and Publications Act 1993

APPENDICES

APPENDIX ONE – Access to business information system

APPENDIX ONE

ACCESS TO BUSINESS INFORMATION SYSTEMS

Information contained in specific business information systems is subject to additional security protocols, due to the personal and potentially confidential nature of the information. Access to the NMIT systems requires written authorisation both from the nominated System Administrator and Line Manager of the individual requiring access. Individuals are assigned to roles within the systems appropriate to their level of seniority/job role/expenditure levels, as determined by the two authorising parties and overseen by the Directorate.

Responsibilities for controlling user access to NMIT's Business Information Systems and authentication are listed in the table below. This list covers all NMIT Information Systems in use at the time of this Policy update. This Policy also covers any new Information Systems subsequently introduced or utilised by NMIT.

The System Administrator is primarily responsible for determining which level of authentication/login is appropriate, advised by ITCS:

Business Function	**System**	**Area responsible for System Administration**
Asset Management	SMP	Campus Services
CCTV	Milestone	Campus Services
Contracts Database	Agiloft	Information Management
Employee Email	Office 365 Outlook	ITCS
Enquiries Management	DeskPro	Customer Success Team
File Storage	Office 365 OneDrive Shared Drives	ITCS
Financials/Purchase Ordering	TechnologyOne UniMarket	Finance
Human Resources	Leader Kiosk Snaphire	POD (People and Organisation Development)
ID Cards & Room Access	Cardax	Campus Services
Library	Liberty	Learner Services
NMIT Council Records	BoardBooks	CE Office
NMIT Intranet	Polly (ElcomCMS)	Intranet & Digital Workplace
NMIT Public Website	Silverstripe CMS	Customer Success Team
NMIT Student Portal	MyNMIT	Customer Success Team
Online Learning	Moodle	LII (Learning Innovation and Insights Team)
Student Management	ebs client ebs ontrack ebs windows eTrack	ITCS
Transport Booking	iJourney	Campus Services