Government of Western Australia
North Metropolitan TAFE

Information Services Acceptable Use Policy (Student)

PCY054

Effective: November 2022

Version: 2.4

Note: this document is available in alternative formats upon request including electronic or audio format.

Contents

All policy and procedural statements contained within this document are lawful orders for the purposes of section 80(a) of the Public Sector Management Act 1994 (WA) and are therefore to be observed by all College employees.

Policy Statement

This policy assists students to make appropriate use of the North Metropolitan TAFE (NMT) Information and Technology (IT) resources and to inform students of the consequences of misuse.

All students using the NMT IT services are required to comply with the principles outlined in this policy. In using Information Technology, all students have a right to be treated fairly and have an obligation to act responsibly.
Inappropriate use exposes NMT and the Student to various risks including but not limited to malicious attacks, malware, and compromise of network and computer systems leading to reputational or legal ramifications.

Scope

This policy applies to all students of NMT. They are responsible for exercising good judgement regarding appropriate use of information, electronic devices and network resources in accordance with the NMT policies and standards and local laws and regulations.

Principles

The following overarching principles are to be followed by all students with access to the NMT systems or data.

1. **Training first**
   IT assets and services are made available to students for education and training purposes. Limited personal use is permitted provided it does not impact on training delivery. They are not to be used for commercial purposes.

2. **Protect NMT interests**
   IT services should not be used in a way that could cause the organisation embarrassment or loss, or to promote interests other than those of the NMT.

3. **Approved components**
   Only authorised equipment, software, and services can be introduced and used in NMT's environment. Personal devices can be connected to NMT guest wi-fi network. Students are responsible for the protection and upkeep of their own equipment and software, and safeguarding the use of their accounts.

4. **Lawful use**
   IT assets and resources can only be used for lawful activities, and cannot be used for any activities which would contravene any laws or regulations with which NMT is obliged to comply.

5. **Report Issues**
   If you believe or suspect that something is not secure, or you need advice please promptly inform your lecturer or other NMT staff member, who will report the issue to the IT Support Helpdesk IT@nmtafe.wa.edu.au.

6. Unacceptable uses of IT services

Unacceptable use includes, but is not limited to the following. Students must not:

a. use another student's digital identity, nor must you attempt to find out the password of another student, allow another person to use your digital identity, share passwords or leave your device unsecured.
b. attempt to subvert security measures in any way e.g. undertake any activities that could result or assist in the violation of any NMT policy, software licence or contract. Examples of these prohibited tools include viruses, trojan horses, worms, password breakers, network packet observers or sniffers. Examples of prohibited activities include creating ping floods; spoofing packets; performing denial-of-service attacks; forging routing information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.
c. must not deliberately circumvent any precautions taken to prevent malicious code accessing College systems e.g. by disabling antivirus software.
d. attempt to adversely interfere with the operation of any of NMT IT services. For the purposes of this document, interfering includes wilful physical damage, wilful destruction of information, and wilful interruption of normal operations, theft and accessing restricted areas.
e. wilfully waste IT services e.g. wasting network bandwidth by downloading, printing or sending large amounts of material that is not study-related.
f. use IT services to send obscene, offensive, bogus, harassing or illegal messages.
g. use the NMT IT services for commercial purposes nor publish or circulate information about other organisations via the NMT IT services.
h. use the IT services in a way that would be considered to pose cyber threat or social engineering risk to NMT or any other party.
i. intentionally create, view, transmit, distribute, copy or store pornography or objectionable material via NMT IT services.
j. intentionally create, view, transmit, distribute, copy or store any information, data or material that violates Australian legislation (including federal legislation or Western Australian state legislation). For example, you must not view, store, send, or give access to material regarded as objectionable by the Western Australian Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40 (e.g. sexually explicit material involving children, incitement to violence, torture, and bestiality).
k. attempt to conceal or erase the evidence of a breach of NMT IT security.
l. allow your computer or personal devices to adversely affect NMT's IT services if you are bringing your own devices to campus and utilising wireless network services provided by NMT.
m. leave personal information stored within NMT IT services after your enrolment ceases. You must make arrangements for its retention and/or removal as appropriate prior to cessation of your enrolment
n. Use the College ICT network for the purpose of copyright infringement. If you are found to be repeatedly engaging in activities contrary to this policy, your ICT network access privileges may be suspended.
o. Connect to NMT services using a public VPN.

7. Compliance

To ensure student compliance with this policy, NMT reserves the right to verify compliance to this policy through various means including but not limited to monitoring student IT service activity and usage, reviewing logs and engaging

internal and /or external audit. Students acknowledge that their usage may be monitored.

8. Non compliance

a. Any student found to have violated this policy may be subject to disciplinary procedures as outlined in Part 6 of the North Metropolitan TAFE By-laws.
b. NMT may terminate a student's IT service access and/or notify the relevant authorities if NMT staff believe that a breach has occurred.
c. NMT may impose further sanctions, as outlined in the Student Code of Conduct.
d. Sanctions applied in non-IT areas may result in removal of IT services to students

Background

NMT is committed to protecting its employees, partners, students and the organisation from illegal actions by individuals, either knowingly or unknowingly. IT resources are to be used in a responsible and accountable manner that ensure the efficient, effective and acceptable use. Additionally, students are aware that they are bound by the NMT Code of Conduct which has provisions for the proper use of official information, equipment and facilities.

NMT provides students with the following IT services for learning and research purposes, during their enrolled unit, course or pathway of study:

- access to computer software and equipment
- access to wireless network services
- access to the Internet
- access to email

All IT systems, including but not limited to computer equipment, software, operating systems, storage media and network infrastructure are the property of NMT. These systems are to be used for business purposes in serving the interests of the organisation and of our customers during normal business operations.

Effective information security is a team effort involving the participation and support of every User who deals with information and/or information systems.

For further information on cyber security, please refer to: https//staysmartline.gov.au

Under the Criminal Code Act (1995), it is an offence to use the internet, social media or a telephone to menace, harass or cause offence. The maximum penalty in this offence is a three year imprisonment or a fine of more than $30,000.

Information on how to report cyber bullying and illegal content can be found on the eSafety Commissioner's website: https://www.esafety.gov.au.

Definitions and Acronyms

Term	Definition
Virus	A computer program that can infect other computer applications or system areas by modifying them to include a copy (possibly modified) of itself.
Malware	Unwanted or malicious software e.g. worms, Trojan horses, bots.
Worms	A worm is a program that makes copies of itself (usually one per system) across a network. It may do damage and compromise the security of a computer, but it doesn't replicate by changing a hosts code or files. Viruses infect, worms infest.
Trojan horses	A Trojan Horse is a program that does something that its programmer intended but the user is not expecting. Viruses must replicate to be classed as viruses, Trojans do not replicate.
Packet sniffers	A sniffer (packet sniffer) is a tool that intercepts data flowing in a network.
Ping floods	A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with Internet Message Control Protocol (ICMP) echo request (ping) packets.
Spoofing packets	Involves masking the IP address of a certain computer system.
Denial-of-service	A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
Honeypots	A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.
Honey net	A network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated.

Related Policies and Other Relevant Documents

- Information Services Information Security Policy (PCY052)
- Student Code of Conduct
- Disciplinary Procedures – Part 6, NMT By-laws

Review Date

Nov 2024

Contact Information

Director Information Services

Revision History

Version No.	Approved/ Amended/ Rescinded	Date	Approval Authority	Amendments

2.0	Approved	Sept 2018	ITC GC CORPEX	
2.1	Amended	April 2020		Added point (m) - Update information on copyright in line with safe harbour scheme
2.2	Amended	Nov 2020	Director Information Services	Review and update of policy and terms
2.3	Amended	Nov 2022	Director Information Services	Review and minor updates