Acceptable Use Policy

Audience and scope:

This policy is relevant to all staff, students and other users of computer systems owned or managed by Manukau Institute of Technology Limited (MIT).

Document management and control

Policy Number	ICT1	**Consultation Scope**	Executive Leadership Team
Category	Management	**Approval Bodies**	Chief Executive
Policy Owner	DCE Operations	**Review Dates**	March 2024
Policy Contact Person	Head of Technology Services		

Amendment history

Version	Effective Date	Created/Reviewed by	Reason for review/Comment
.001	31st May 2016	Melanie Visser	New Policy
.002	22nd February 2018	Russell Smith	Review, update and migrate to new template
.003	20th March 2018	Russell Smith	Review by Legal
.004	10th July 2018	Manette de Beer	Amended based on feedback from Chris Park – Academic Registrar
.005	15th November 2019	Manette de Beer	Amended based on feedback from EGM People and Culture
.006	11th February 2020	Manette de Beer	Updated to include eSignatures
.007	7th October 2020	Jenna Woolley	Updated to include preferred names
.008	22nd March 2022	Ricky Oliver	Review, update to reflect new Executive leadership structure

Table of Contents

Acceptable Use Policy

Purpose

This policy applies to all members of the MIT community whether at MIT or elsewhere, and refers to all Information Technology (IT) resources.

The policy defines the responsibilities of all IT users to use and to protect IT resources appropriately.

Policy

MIT provides IT resources to a large and varied group of users. All users have a responsibility to use these resources in an effective, efficient, ethical, and legal manner.

Ethical and legal standards that apply to IT resources are based on the standards of common sense and courtesy that apply to any shared resource. These resources are supplied on the understanding that IT users act as good citizens and that they contribute to creating and maintaining an open community of responsible users.

Members of the MIT community must at all times comply with relevant laws, and MIT or Te Pūkenga statutes, policies and standards. IT users who deal with sensitive data must take particular care to ensure that they comply with all laws and MIT policies and practices relating to the privacy and security of data. Some units within MIT, including Technology Services and Academic Centre, maintain additional IT standards. IT users to whom those additional standards apply must also comply with those requirements.

MIT seeks to establish and maintain access for its community to local, national and international sources and works to create an environment in which staff and students feel free to create and to collaborate with colleagues both at MIT and at other institutions, without fear that their work will be misrepresented, tampered with, destroyed or stolen.

Procedures

1. IT User Obligations

1.1. MIT's IT resources are to be used in a way that is consistent with MIT's teaching, learning, public sector, research, administrative objectives and any specific objectives of projects or tasks for which use is authorised.

1.2. IT users must use IT resources responsibly, efficiently and in an ethical manner, and with due regard to the rights of others. IT users must not engage in any illegal activities or purposes, whether knowingly or unknowingly.

1.3. All IT users must not engage in and must guard against any misuse or activity which aims to disrupt or damage IT resources at MIT or beyond.

1.4. IT resources are provided for business and/or academic purposes. Any personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring MIT into disrepute.

1.5. For the avoidance of doubt, unacceptable conduct by IT users includes, but is not limited to:

(a) using IT resources in a way that interferes with the reasonable use of IT resources by other IT users;

(b) using IT resources in a way that hinders MIT in meeting its legal obligations;

(c) assuming another person's identity or role, including using another person's electronic signature, login or IT access;

(d) communicating on behalf of an organisation or unit that the IT user does not have the authority to represent;

(e) accessing, using, destroying, altering, dismantling or disfiguring IT resources without appropriate authority or other lawful excuse;

(f) breaching any intellectual property rights of MIT or any third-party copyright or patent protection and authorisations, including license agreements and other contracts;

(g) breaching the privacy of individuals without appropriate authority or other lawful excuse; and/or

(h) using IT resources to bully, harass or victimize any other person.

2. Monitoring

2.1. In order to comply with MIT policy requirements, monitoring of the use of MIT computer systems (including but not limited to Sharepoint and Onedrive), will be undertaken. This will apply whether MIT systems are accessed at a MIT site, at home or any other location. Without limitation, monitoring may include:

(a) the content and usage of email;

(b) internet usage and participation in discussion forums;

(c) email and internet usage;

(d) usage data such as account names, source and destination accounts and sites;

(e) dates and times of transmission or access;

(f) size and/or content of transmitted material;

(g) other usage related data; and/or

(h) remote access.

2.2. Information obtained may be used for the purposes of accounting, troubleshooting and systems management, and where appropriate preventative or disciplinary action.

3. Disclosure of Information

3.1. All information created and/or stored on MIT's IT resources may be subject to disclosure by MIT under freedom of information legislation such as the Official Information Act or the Privacy Act, or in the course of the discovery process if there is litigation in progress

4. Use of Electronic Signatures (eSignatures)

4.1. MIT has a strict policy around the use of electronic Signatures. All users will ensure that:

a) When electronically signing a document, that only embedded signatures from MIT's approved pdf providers are used;

b) All electronic signatures are securely stored and that devices these signatures are stored on are password or pin protected and locked when not in use;

c) Electronic signatures are not misused. Any misuse of electronic signatures (whether your own or another person's electronic signature) is fraudulent behaviour that will constitute a breach of MIT's policies and/or applicable laws.

5. Preferred Names

5.1. Except where the legal name is required by law, MIT will allow users to use a preferred name to reflect their digital identity, ie display name within systems while working or studying at MIT. This can be requested via the MyMIT Self Service Portal for staff and by logging a request via MITHub or via AskMe! for students. Provided that the preferred name change request meets the criteria outlined in this section a change will be made to display the preferred name. Official documentation issued by MIT must use the full legal name. Preferred names must not be offensive, longer than 30 characters (including spaces), an official title or rank or resembling one,

or spelled with numbers or symbols. Users may only change their preferred name once during their period of enrolment or employment. Any further name changes will be referred to the General Manager Academic Services, or Director, People and Culture for consideration and should be supported by an appropriate explanation or evidence.

Failure to follow this policy

Failure to follow any part of this policy may result in MIT undertaking disciplinary action in accordance with its Disciplinary Policy

Evaluation/Outcomes

Audit: The Risk and Assurance Manager may audit compliance with this policy as part of internal audit work programmes.

Compliance: The policy owner will monitor compliance.

Additional Information

Glossary

Term	Definition
Academic Freedom	The right of teachers and students to express their ideas in the classroom or in writing, free from political, religious, or institutional restrictions, even if these ideas are unpopular.
Intellectual Property	Proprietary rights concerning all original work governed by the Copyright Act 1994, the Patents Act 1953, the Designs Act 1953, the Trade Marks Act 2002, the Layout Designs Act 1994, the Plant Varieties Act 1987, any amendments to these or subsequent acts and any other intellectual property law. It includes, but is not limited to: • Course materials. • Research data and outputs. • Assessment materials. • Administrative materials. • Computer software, videos and recordings. • Creative, literary works, artwork. • Discoveries/innovations/inventions. • Patents, Copyright, designs, trademarks. • Patentable and potentially patentable subject matter and associated know how. • Plant variety.

Exemptions and dispensations

Any dispensations from the requirements of this policy, including any one-off circumstances, must be approved in writing by the Chief Executive and the DCE Operations.

Delegations

- Board Register of Permanent Delegations and Authorisations.
- Statute 2: The Delegations and Authorisations Statute.
- Delegated Authorities Policy (FIN2).

Relevant Legislation

- Copyright Act 1994.
- Privacy Act 2020.
- Education and Training Act 2020.
- Human Rights Act 1993.
- Harassment Act 1997.

Legal Compliance

This policy complies with MIT's statutes, regulations and relevant legislation.

Associated documents

The following documents are associated with this policy:

- Student Misconduct Policy (AM6).
- Intellectual Property Policy (AM10).
- Delegated Authorities Policy (FIN2).
- Procurement Policy (FIN3).
- Disciplinary Policy (HR7).
- Harassment, Discrimination and Bullying Policy (HR14).
- Email Policy (ICT3)
- Internet Usage Policy (ICT4)
- Mobile Device Policy (ICT5)
- Fraud Prevention and Response Policy (LC2).
- Records Management Policy (LC4).
- Information Act Requests Policy (LC5).
- Privacy Policy (LC6).
- Bring Your Own Device Guidelines.
- Employee Acceptance Form.
- Application for Remote Access Form.
- Remote Access Agreement.
- Lost, stolen and damaged devices procedure (staff)
- Lost, stolen and damaged devices procedure (student)