Acceptable Use Policy

Audience and scope:

This policy is relevant to all staff, students and other users of computer systems owned or managed by MIT and EnterpriseMIT.

Document management and control

Policy Number	ICT1	**Consultation Scope**	Senior Leaders, Leadership Team
Category	Management	**Approval Bodies**	Chief Executive
Policy Owner	CFO and Director Corporate Services	**Review Dates**	January 2017
Policy Contact Person	Head of ICTS		

Amendment history

Version	Effective Date	Created/Reviewed by	Reason for review/Comment
.001	30 November 2015	Melanie Visser	Created new policy.
.002	4 February 2016	Melanie Visser	Updated document with feedback from ICTS Management, Legal, People & Culture
.003	21 March 2016	Melanie Visser	Updated document with feedback from first round of consultation.
.004	30 March 2016	Melanie Visser	Updated document with feedback received from Leadership Team.

Table of Contents

Acceptable Use Policy

Purpose

The purpose of the Acceptable Use Policy is to ensure that all computer systems and networks owned or managed by MIT are operated in an effective, safe, ethical and lawful manner. It is the responsibility of every computer user to know these requirements and to comply with them.

Policy

MIT will implement the following controls across its computer systems and networks:

1. Access Control

1.1 Rights are granted on the basis of business need and access to relevant systems is provided by the appropriate system administrator. Any other access is considered unauthorised and is in breach of this requirement.

Misconduct will be handled in accordance to MIT's Disciplinary Policy.

1.2 MIT supports Bring Your Own Device (BYOD) on our wireless network. However, the use of personal mobile phones, tablets, portable computers, laptops etc must comply with the requirements outlined in ICTS' BYOD Guidelines.

1.3 Damaging, altering, or disrupting the operations of the computer systems and networks owned or managed by MIT is not permitted. Users must not carry out any activity with the intention of capturing or obtaining passwords, encryption keys, or anything that could facilitate unauthorised access by themselves or anyone else.

1.4 Before a user reaches a menu, system prompt or has access to system resources, utilities, databases or shares they must have successfully logged on and be validated as a legitimate system user. Authentication methods will depend on the sensitivity of the information or system being accessed, whether access is effected in-house or remotely and the level of privileges granted to the user.

2. Anti-Virus

2.1 Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise affect the performance of, or access to any MIT computer system or network.

3. Communication and Mobile Devices

3.1 Mobile devices and communication systems supplied by MIT are provided to facilitate business activities. Personal use is permitted provided it is reasonable and appropriate.

Directors/senior managers will monitor use and are provided with monthly reports. Personal use may be required to be reimbursed.

A phone or phone number supplied by MIT may not be used in connection with any personal commercial business activities. The number may not be published in any publication or business card that is not related to MIT's business.

3.2 Mobile devices and communication systems owned or managed by MIT are to be used in an effective, safe, ethical and lawful manner. Use will be monitored and misuse will be handled in accordance with MIT's Disciplinary Policy.

3.3 Users of MIT's mobile phones and communication systems must not engage in any activity which violates or infringes the rights of others or which a reasonable person would consider to be abusive, indecent, offensive or defamatory.

Any such activity will be handled in accordance with MIT's Disciplinary Policy.

3.4 Communications equipment supplied by MIT must not be altered or added to in any way including:

- Unauthorised upgrades.
- Addition of components.
- Removal of components - including transferring an MITSIM card to a personal phone.
- Altering configuration or security settings.
- Installation of non-approved applications.
- Jailbreaking the device.

All devices will be centrally managed and any changes or maintenance will be carried out by the ICTS Service Desk or designated agent.

3.5 Users of mobile devices supplied by MIT must ensure that the device is protected by a PIN number or password and auto-lock. Voice authentication (if used), must be coupled with password or PIN authentication.

3.6 MIT maintains the right to conduct inspections of any mobile phone or other mobile device that it owns or manages without prior notice to the user or custodian. The device must be returned to the ICTS Service Desk upon request for maintenance and when the user ceases to provide services to MIT.

3.7 Users should not lend mobile devices allocated to them for business activities to anyone. This includes co-workers, friends and family.

3.8 Staff using communications devices must not return calls, text messages, respond to pager calls or subscribe to paid services where:

- A call or other response does not relate to business purposes and where charges beyond those for normal calls can be incurred (e.g. long distance calls).
- The return number has an 0900 area code.
- The recipient is a competition, gambling or advertising entity.
- Charges will be reversed back to MIT.

Any costs incurred relating to the above will be the responsibility of the staff member.

3.9 With the exception of purchases made from an approved online application store (e.g. Apple's App Store or Google's GooglePlay), games, freeware, shareware, movie clips or music may not be downloaded onto any MIT mobile device unless its use is legal (does not breach copyright law). Movie clips taken with the device for work purposes are exempt from this requirement.

3.10 Skype for Business is the only approved enterprise voice and video communication system. Any other voice and video communication system must be approved by the Head of ICTS.

Voice and video communication is to be used for business purposes. Personal use is permitted provided it is reasonable and appropriate.

Voice and video systems are not to be used for the following:

- Commercial announcements.
- Advertising material.
- Sexually explicit or sexually oriented material.
- Hate based material.
- Hacker related material.
- Transferring of files.

All inbound and outbound communication must be channelled through corporate systems and accounts.

4. Computer Systems and Equipment Use

4.1 Users of computer systems or networks owned or managed by MIT shall not use these systems to engage in any activity which contravenes human rights legislation or which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user for any reason or on any grounds, including on any prohibited grounds.

Any such activity will be handled in accordance with MIT's Disciplinary Policy.

4.2 The computer systems and networks of MIT are primarily for business use and must not be used for illegal or unethical purposes in any circumstances. Illegal or damaging actions or activities whether performed knowingly or unknowingly, constitute misconduct and will be handled in accordance with MIT's Disciplinary Policy.

4.3 The computer systems are to be used for business purposes in the course of normal day to day operations. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring MIT into disrepute.

4.4 MIT supports Bring Your Own Device (BYOD) on our wireless network. However, the use of personal mobile phones, tablets, portable computers, laptops etc must comply with the requirements outlined in ICTS' BYOD Guidelines.

4.5 USB sticks, key fobs or any other storage devices allocated by MIT are are only for business use. Extra care is required when storing information on these devices due to their size and portability. Users should be aware of the following:

- Loss of keys and data is a problem due to the small size of these devices.
- Increased chances of introducing a virus as such devices can be used on multiple computers.
- Such devices should not be inserted into any computer that does not have up to date security patches and anti-virus software.
- Such devices must be stored and transported in a safe manner to reduce the chances of loss.
- Data on such devices should be encrypted.
- Such devices found at random should not be used at all. Such devices should be handed into ICTS immediately.

4.6 Computer equipment supplied by MIT must not be altered or added to by users any way including:

- Unauthorised upgrades.
- Addition of components.
- Removal of components.
- Altering configuration or security settings.
- Installation of non-approved applications.

All changes to configuration or maintenance of the device must be carried out by ICTS staff or their designated agent.

4.7 Users should not lend computers, portable devices, tablets, mobile phones laptops or any other equipment that has been allocated to them by MIT for business activities to anyone. This includes, co-workers, friends and family.

4.8 Any actions or activities, whether intended or accidental which cause, or could cause the computer systems, information or networks of MIT to be compromised in any way is considered serious misconduct including (but not limited to):

- Security breaches or disruptions of network communications. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
- Port scanning or security scanning. These activities are expressly prohibited unless sanctioned by the Head of ICTS for the purposes of testing network security.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal duties or has been duly authorised.
- Circumventing user authentication or security of any host, network or account or running password cracking programs.
- Interfering with, or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally.
- Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data.
- Copying or altering configuration or system files for unauthorized personal use or to provide to other people or users for unauthorized use.
- Creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with MIT’s or another organisation's email service.
- Downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by MIT or not.
- Providing or selling MIT information without approval and for personal gain
- Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using MITresources that would bring MIT into disrepute.

4.9 Users must use the standard applications for which MIT is licensed. Users are not permitted to install any software program, application, script or executable code on MIT equipment in their care. Only software approved by the Head of ICTS may be installed on MIT equipment.

Where applications, programmes, scripts or code is needed for a specialist lab or teaching environment, such downloads should be performed by an authorised faculty staff member.

4.10 Users working in MIT's premises are not permitted to connect to the Internet using mobile USB modems, personal hotspots, USB mobile wireless devices, mobile broadband cards or any other mechanism that bypass official corporate systems.

Devices provided by MIT have been configured to connect to network resources (including the Internet) using approved wired or wireless mechanisms.

Use of mobile computing facilities may only be used remotely.

4.11 If printing confidential or potentially sensitive information the following must be observed:

- The person authorised to view the information, or that person's authorised representative, must be present at the printer during printing to ensure no one else reads the document; or
- The printer is located in a secure area; or
- The document is printed to a storage area on the printer and a code entered or card swiped to initiate the print when the authorised person or their representative is present

The same applies to scanners, fax machines and photocopiers.

5. Email

5.1 The email system is predominantly for business use. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring MIT into disrepute.

Misuse will be handled in accordance with existing MIT Disciplinary Policy.

Refer to section 1.1 of the eMail Policy.

5.2 The email system must not be used for any unlawful activity and must not be used to compromise the security or operation of any computer system or network whether it is owned or managed by MIT or not.

Any such activity will be handled in accordance with MIT's Disciplinary Policy.

Refer to section 1.5 of the eMail Policy.

5.3 Users of email systems owned or managed by MIT shall not create, send or forward any email that contravenes human rights legislation or which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user for any reason or on any grounds, including on any prohibited grounds.

Any such activity will be handled in accordance with MIT's Disciplinary Policy.

Refer to section 2.4 of the eMail Policy.

5.4 The email system is regarded as an official means of communication and, as such, messages must conform to the same corporate rules for grammar and content as other business communications.

It is not appropriate to use abbreviations (as used in text messages) or profanities, obscenities, derogatory or sexually explicit remarks in business email messages. Such remarks, even when made as a joke, may upset some people. Special caution is warranted because backup and archival copies of email may be more permanent and more readily accessed than traditional paper communications.

Refer to section 2.5 of the eMail Policy.

5.5 MIT has a legal requirement to retain corporate email. Users should regularly move corporate emails from email folders to the appropriate information repository.

Corporate email is defined as:

- eMail that forms part of the corporate record. It is email that documents the business activities of MIT, e.g. a direction for an important course of action, business correspondence received from outside MIT or a communication between staff members in which a formal approval is recorded.

Ephemeral emails can be destroyed as part of normal administrative practice.

Ephemeral email is defined as:

- eMail used to facilitate MIT's business but which does not need to be retained for business purposes, e.g., notice of meetings, staff movements, copies of reports or newsletters, advertising material and any other publicly available material.

Personal email should be destroyed as soon as it is no longer required.

Personal email is defined as:

- eMail of a personal nature that has no relevance to the business of MIT.

Refer to section 3.1 of the eMail Policy.

5.6 Staff email will be backed up and archived in accordance with MIT's Records Management Policy.

Backups take place daily and are kept for approximately three months.

Mail is archived indefinitely.

To minimize the size of the backups, staff sent and deleted emails older than a year are deleted from the user's respective folders. Staff can access these items through the archive functionality.

Student email is not backed up or archived by MIT.

Refer to section 3.2 of the eMail Policy.

6. Information Management

6.1 Subject to any third party agreement, any document, data and/or information created modified saved, transmitted or archived using the corporate systems of MIT, or otherwise located within a computer system owned or managed by MIT, remains the property of MIT. For the avoidance of doubt, this includes any personal documents and emails.

6.2 All corporate information and data must be stored in approved corporate information repositories. This includes the appropriate information repository, corporate applications and other approved shared repositories. Information is not to be stored on local drives of PCs or workstations, USB devices, laptops or copied onto portable media such as CDs or DVDs unless these copies are made in addition to saving it in an approved corporate file system.

6.3 Electronic information must be protected based on its sensitivity, value and criticality regardless of the type of media that holds the information, its location, the systems used to process it or the processes it is subjected to.

6.4 The user must notify their manager immediately if confidential or sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed.

6.5 Users must not delete or dispose of potentially important MIT electronic records or information without the approval of the information owner and without following standard document management procedures for disposing of information.

Deleting MIT's records without following the proper procedures is considered a serious breach of this requirement particularly if the records cannot be recovered. Such actions will be handled in accordance with MIT's Disciplinary Policy.

It should be noted that document retention should be in accordance with MIT's Records Management Policy and the Archives New Zealand Standards.

7. Internet Use

7.1 The internet is primarily available for business use. Personal use must be reasonable and appropriate, not impact on staff productivity or system performance or bring MIT into disrepute.

A web content control system monitors and controls website visits.

Misuse will be handled in accordance with MIT's Disciplinary Policy.

Refer to section 1.1 of the Internet Policy.

7.2 MIT monitors and logs websites visited, files downloaded and social networking accounts. Directors/senior managers can request reports that allow them to monitor and moderate internet usage. Users viewing or downloading content that is deemed inappropriate for the workplace will be subject to the applicable actions as defined by MIT's Disciplinary Policy.

Refer to section 1.2 of the Internet Policy.

7.3 Users of the internet connection managed by MIT shall not use the connection to visit, interact with, or download content from websites that are offensive, obscene, contain indecent material (such as pornography and violence), contravene human rights legislation or which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user for any reason or on any grounds, including on any prohibited grounds.

Any such activity will be handled in accordance with MIT's Disciplinary Policy.

Refer to section 1.4 of the Internet Policy.

7.4 The internet connection must not be used for any illegal or unethical activity or personal business activity and must not be used to compromise the security of any computer system or network whether owned or managed by MIT or not.

Misuse must be reported to a director/senior manager or People & Culture immediately. Reports of misuse will be investigated and handled in accordance to MIT's Disciplinary Policy. Examples of unacceptable internet use include (but not limited to)

- Computer hacking (accessing another's electronic data or computer without permission).
- Providing access to unauthorised persons (including minors).
- Impersonation.
- File downloads (except for work related reasons).
- Use of the internet for personal gain.
- Gaming, wagering or betting.
- Playing games.
- The intentional transmission in any way of viruses or files that cause a negative impact on computer systems (e.g. unauthorised email attachments such as video, audio and executable files).
- Downloading or distributing information subject to copyright requirements (such as licensed software or protected internet applications).
- Disclosing private or confidential information including passwords or other information that may compromise the security of the computer systems.
- Engaging in any illegal activity, including dissemination of material in breach of legislation.
- Bypassing MIT's security, fire walls and authentication mechanisms.

Refer to section 1.5 of the Internet Policy.

7.5 Peer to peer file sharing is not permitted. This requirement includes (but not limited to) sharing or downloading of movies, music, ebooks, applications, games and so forth.

Refer to section 1.6 of the Internet Policy.

7.6 When working on their device within MIT's premises, users must use one of MIT's internet connections provided. Users must no circumvent internet security by using USB modems, personal hotspots, USB mobile wireless devices and mobile broadband cards.

Use of such alternative methods of connecting to the internet onsite must only be used for testing purposes and must be approved by the Head of ICTS prior to being used.

Refer to section 1.8 of the Internet Policy.

7.7 The internet shall not be accessed from another employee's PC, unless the user is logged on with their own user name and password.

Refer to section 1.12 of the Internet Policy.

7.8 Membership of, or contribution to social networking groups representing MIT must be in accordance with MIT's Social Media Policy [under development]. Use of social media is not a right for all employees and must therefore be used in accordance with the aforementioned policy. This includes but not limited to:

- Social networking sites including Facebook, Bebo, MySpace, Friendster, Twitter.
- Video and photo sharing sites including YouTube, Flickr, Google Picasa Web, Photobucket.
- Collaborative information sites including Wikipedia.
- Social news sites including Digg, Reddit.

Personal use of social media sites is permitted as long as use is reasonable, appropriate and does not impact on staff productivity or system performance.

If unreasonable personal use or misuse is identified, those rights will be rescinded.

Participation in work related social media groups, chat groups, list servers or collaborative sites must be conducted in accordance with the Social Media Policy.

Refer to section 2.1 of the Internet Policy.

7.9 Users must not use social media to cause annoyance or anxiety, to harass, to defame or to transmit unsolicited commercial or advertising material. These actions must be reported to a director/senior manager or People & Culture immediately. Such actions will be handled in accordance to MIT's Disciplinary Policy.

Refer to section 2.2 of the Internet Policy.

7.10 Unless used for academic or business purposes, employees are not permitted to create or maintain a blog, wiki or social networking site on behalf of MIT without the express permission of the Director of Sales and Marketing. Any blog, wiki or shared workspace must have a moderator and approved code of conduct.

Refer to section 2.7 of the Internet Policy.

8. Legal Compliance

8.1 Users must not disclose any confidential information belonging to MIT or otherwise coming into their possession during the course of their employment, except as expressly permitted under any of the MIT's policies or as required by law. Users may be required to sign a confidentiality or non-disclosure agreement. Information may be classified as follows:

- Not to be stored - Information which may not be captured or saved in electronic systems.
- Confidential - Information restricted to a small number of people.
- Internal Use Only - Information which may be known by staff, but not by anyone external to MIT.
- Public - Information that is approved for public dissemination.

8.2 All intellectual property (including patents, copyrights, trade marks, inventions, designs or other intellectual property) created and/or developed by the MIT's employees while at work or while using the MIT's equipment shall be subject to MIT's Intellectual Property Policy.

8.3 Third party software in the possession of MIT must not be copied or installed multiple times unless this is allowed by the licence agreement. In all other cases the number of installations should be equal to the number of licences held. Systems will be monitored to ensure software licence conditions are being complied with and licence numbers are not being exceeded.

8.4 Information that constitutes 'personal information' and is held in all computer systems and networks owned or managed by MIT is subject to the provisions of Privacy Act 1993 and MIT's Privacy Policy and users should be aware of their obligations in respect of managing and using personal information and providing personal information to third parties.

9. Online Services

9.1 When using the MIT's computer systems, or when conducting MIT's business, staff must not deliberately misrepresent themselves and, where possible, provide full contact details.

9.2 Unless approval has been obtained in advance from a director or senior manager, users are prohibited from establishing online business to business arrangements or signing up to online services provided via the internet.

Where the online system involves payments or receipts, a secure platform for processing transactions must be approved. Examples include (but are not limited to) electronic purchasing, personnel management systems, online database services, Drop Box, iCloud, Skype etc.

Requests for a new online business channel or online service should be made on the New Computer Initiative Request template on MITDesk.

Any online purchases by MIT staff must comply with the requirements for online purchasing set out in MIT's Procurement Policy.'

Financial transactions transacted online must comply with legal requirements, be within approved limits of delegated authority for expenditure and meet the requirements MIT's financial auditors.

Refer to section 1.9 of the Internet Policy.

9.3 Users must not publish corporate information (applications, internal documents or files, press releases, price lists etc.) on any public facing computer system (e.g. website, social media site) unless the item has been authorised by Sales and Marketing for public consumption.

10. Password and Authentication

10.1 User IDs and passwords must not be disclosed to anyone or shared with anyone.

Group or generic User IDs and passwords are prohibited as a rule, but in special circumstances may be approved by the Head of ICTS who will keep a written record of the exceptions.

10.2 Passwords must not be written down and left in a place where unauthorized persons might discover them.

10.3 Staff that use a personal computer at home should use different login credentials for their work and home accounts.

10.4 Users are responsible for all activity performed with their personal user IDs and passwords. Users must not allow others to perform any activity with their user IDs and are not permitted to perform any activity with IDs belonging to other users.

11.0 Personnel Management

11.1 All breaches of ICTS policies and guidelines by staff members will be handled by People & Culture in accordance with MIT's Disciplinary Policy.

Breaches of ICTS policies and guidelines by students will be handled in accordance with MIT's Student Misconduct Policy.

12. Remote Access

12.1 Citrix is the preferred remote access portal. All staff have access to Citrix by default.

Users (staff or external users) who require access to the virtual private network (VPN) must log a request on MITDesk and obtain approval from the Head of ICTS.

Remote users are only permitted access to applications and systems they have been approved access for the purpose of fulfilling obligations to MIT. All other access is unauthorised.

No VPN access is permitted unless:

- The request is logged on MITDesk.
- The request is approved by ICTS management.
- The Remote Access Agreement has been signed.

12.2 Users must not be remotely connected to MIT while concurrently connected to another network or initiate a connection to another network during the period they are connected to the MIT. This practice is called split tunneling.

13. MIT's Right to Monitor and Access All Computer Systems

13.1 In order to protect MIT property, people and technology and ensure compliance with legal and statutory obligations, monitoring of the use of MIT Computer Systems 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:

i. The content and usage of email.

ii. Internet usage and participation in discussion forums to:

- Identify inappropriate use.
- Protect system security.
- Maintain system performance.
- Protect the rights and property of MIT.
- Determine compliance with MIT policy.

iii. Network traffic including:

- Email and internet usage.
- Usage data such as account names, source and destination accounts and sites.
- Dates and times of transmission or access.
- Size of transmitted material.

- Other usage related data.

iv. Remote access.

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

13.3 All information created and/or stored on MIT Computer Systems, may be subject to disclosure by MIT under freedom of information legislation such as the Official Information Act, the Privacy Act, or in the course of the discovery progress if there is litigation in progress (please refer to MITNet for relevant policies).

Procedures

Please refer to the policy section.

Evaluation/Outcomes

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

Compliance: The Head of ICTS will monitor compliance.

Additional Information

Glossary

Term	Definition
Approved online application store	Online store created, developed and supported by operating system companies such as Apple, Microsoft, Android.
BYOD	Bring your own device. A methodology whereby staff and students may bring personal devices to connect to MIT systems for learning and business purposes.
Designated agent	MIT preferred supplier.
Intellectual property rights	'Intellectual property' means 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: • Courses 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. MIT data.
MITDesk	MIT's service management system.
MITNet	MIT's intranet.
Prohibited grounds as defined in this policy relate to:	• Race. • Religious belief or activity. • Sex. • Age. • Disability.

	• Industrial association. • Lawful sexual activity/sexual orientation. • Marital, parental or carer status. • Physical features. • Political beliefs or activity. • Pregnancy and maternity. • Personal association with a person who has one of these personal characteristics. • Gender. • Irrelevant criminal conviction.
Reasonable and appropriate use for mobile phones	• Minimal calls and text messages. • The data plan must not be exceeded due to personal use. • Personal use must not cause MIT to incur any additional costs or impact staff productivity.
Reasonable and appropriate use for computer systems	• Minimal personal internet usage. • Minimal personal email usage. • Minimal personal printing. • Personal use must not cause MIT to incur any additional costs or impact staff productivity.
Service management system	System used to log, track and report on incidents, service requests, problems and changes.

Exemptions and dispensations

Any dispensations from the requirements of this policy, including any one-off circumstances, must be approved in writing by the CFO and Director Corporate Services.

Delegations

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

Relevant Legislation

- Copyright Act 1994.
- Privacy Act 1993.
- Unsolicited Electronic Messages Act 2007.
- Education Act 1989.
- Fair Trading Act 1986.
- Harmful Digital Communications Act 2015.
- Human Rights Act 1993.
- Harassment Act 1997.
- Films, Videos and Publications Classification Act 1993.

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).
- Fraud Prevention and Response Policy (LC2).
- Records Management Policy (LC4).
- Information Act Requests Policy (LC5).
- Privacy Policy (LC6).
- Social Media Policy (under development).
- Bring Your Own Device Guidelines.
- Employee Acceptance Form.
- Application for Remote Access Form.
- The Remote Access Agreement.