Internet 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	ICT4	**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 Team, Legal, People & Culture
.003	21 March 2016	Melanie Visser	Updated document with feedback received from first round of consultation.
.004	30 March 2016	Melanie Visser	Updated document with feedback received from Leadership Team.

Table of Contents

Internet Policy

Purpose

The purpose of the Internet Policy is to ensure that the internet is used for business purposes and to ensure that users conduct their online activities in an appropriate, responsible and ethical manner.

Policy

MIT will implement the following controls for internet usage:

User Responsibilities

1. Acceptable Use

1.1 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 7.1 of the Acceptable Use Policy.

1.2 All staff who have a system account have been provided with access to the internet.

1.3 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 7.2 of the Acceptable Use Policy.

1.4 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 7.3 of the Acceptable Use Policy.

1.5 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 7.4 of the Acceptable Use Policy.

1.6 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 7.5 of the Acceptable Use Policy.

1.7 Users must not subscribe to any internet or cloud computing services to host MIT data that are not provided by MIT or regarded as enterprise applications. Any request to use non-MIT approved applications must be submitted to ICTS via MITDesk and approved by the the Head of ICTS. This requirement relates to external data hosting arrangements and the provision of applications using the likes of (but not limited to) iCloud and Dropbox.

1.8 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 7.6 of the Acceptable Use Policy.

1.9 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 9.2 of the Acceptable Use Policy.

1.10 Internet security settings are configured in accordance with MIT's security requirements and must not be changed by users.

1.11 Users are not permitted to download any software, freeware, shareware, application, script, game, music or movie clip or anything containing executable code from the internet using a device connected to the corporate network. If you require something downloaded for business purposes, please contact the ICTS Service Desk.

1.12 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 7.7 of the Acceptable Use Policy.

1.14 Internet voice and video calling facilities such as Skype for Business must be used in accordance with the Acceptable Use Policy and Communication and Mobile Device Guidelines.

2. Use of Social Media

2.1 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 7.8 of the Acceptable Use Policy.

2.2 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 7.9 of the Acceptable Use Policy.

2.3 All reasonable efforts should be made to ensure those representations and other statements made by MIT staff and contractors using social media are not false, misleading, defamatory or in breach of any other applicable laws.

2.4 When contributing to social networking sites a disclaimer or other means should make it clear whether the view expressed is personal or the official position of the MIT.

2.5 Social media users must not infringe copyright or plagiarise another's work. It is important that the appropriate clearances are obtained by the copyright owner prior to publishing online. If copyright clearance is not required and users wish to quote from another source, they must ensure that the source is correctly cited.

2.6 Users must respect the privacy of individuals, and the confidentiality of sensitive or classified information, when publishing online. Users will not post private information about themselves or others, publish confidential information or infringe the intellectual property rights of the MIT. Any use of MIT-owned intellectual property must comply with the MIT's Intellectual Property Policy.

2.7 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 7.10 of the Acceptable Use Policy.

2.8 Posts made on behalf of MIT that are considered business records must be retained, archived and/or destroyed in accordance with the Records Management Policy and any applicable ICTS policies, guidelines and procedures.

2.9 Social media sites that are developed in-house or by third parties for MIT must be signed off by the Marketing Director who approves them for live publishing. This sign off states that corporate standards for presentation, branding, security and usability have been met.

Information, Communication and Technology Services Responsibilities

1. Public facing servers must be locked down in accordance with MIT's security profile to ensure systems are not vulnerable to compromise and the configuration must be fully documented.

2. MIT's domain names must be owned by MIT and registered by the Head of ICTS. The primary internal DNS Server must be the MIT's own DNS server unless approval has been obtained from the Head of ICTS. Where a third party is authorised, a written contract must be signed stating the MIT's service expectations.

3. Remote control access for ad-hoc support such as TeamViewer, Webex, Windows Remote Desktop or Go To My PC is only permitted if approved by the Head of ICTS. If these services are approved, the staff member must remain in control of the PC and in front of it so they can see what actions are taking place.

   Although these are tools which are beneficial for remote support by a third party, they also introduce the following security risks:

   - The third party who has control of the PC is sharing the user ID of an MIT user.
   - The third party invited in may have access to systems and information beyond what they 'need to know i.e. they have access credentials of the user that initiated the session.
   - The third party can record the session and play it back later on.
   - The session is recorded on a server in the USA.
   - Logs record all activities as the user who initiated the session.
   - There is no log entry showing that the third party logged in or out of the network.
   - Unless the session is monitored at all times, MIT cannot be sure what changes were made.

4. A web content control system is installed and configured to monitor and control the browsing habits of users. Logs that record user browsing activities are retained. Websites that are known or suspected as malicious are blacklisted.

5. An Intrusion Prevention System (IPS) is installed to handle malware and malicious code attacks entering MIT through the applicable ports.

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
IPS	Intrusion Prevention System. A system installed on the computer network used to prevent outside attacks and unauthorised access to MIT's networks.
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	ICTS' service management system.
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	• 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).
- Acceptable Use Policy (ICT1).
- Social Media Policy (under development).