eMail 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	ICT3	**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 policy with feedback from ICTS Management, Legal, People & Culture.
.003	21 March 2016	Melanie Visser	Updated policy with feedback obtained from first round of consultation.
.004	30 March 2016	Melanie Visser	Updated document with feedback received from Leadership Team.
.005	31 May 2016	Melanie Visser	Updated document with feedback from Leadership Team.

Table of Contents

eMail Policy

Purpose

The purpose of the eMail Policy is to document how electronic mail systems and services are to be used. eMail is a major communication channel and a common means of conducting day-to-day business. Compliance with this policy is essential to ensure that important email documents become part of the corporate knowledge-base and to ensure compliance with information management and legal requirements.

Policy

MIT will implement the following controls for eMail usage:

User Responsibilities

1. Restrictions of Use

1.1 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 procedures.

Refer to section 5.1 of Acceptable Use Policy.

1.2 Users are provided with remote access to email via the Outlook Web Access (OWA) application or Citrix. These are the only two approved remote systems for email.

1.3 Staff must not use personal email accounts for business use. All business related email must be sent from the MIT domain.

1.4 Sending or receiving email with another staff member’s account, or reading another staff member's email is prohibited unless staff are acting on delegated authority i.e. personal assistants or supervising directors, accessing a former employee’s email or accessing email for audit/disciplinary purposes.

In such cases, delegated authority functions must be initiated by the owner of the email account and rescinded when no longer required.

1.5 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 5.2 of the Acceptable Use Policy.

1.6 Transactions carried out using the email system will be supported by an audit trail providing irrefutable evidence of the transaction that complies with any applicable legal requirement.

1.7 Broadcast facilities found in email systems may only be used for legitimate business purposes when there is a need to communicate one message to a large number of internal staff.

1.8 Distribution groups are to be created and maintained by the ICTS Service Desk.

Requests for such groups are to be made on MITDesk.

New distribution groups will only be added with the authorisation of a director/senior leader or Head of ICTS. Distribution groups should only be created for business purposes. Distribution groups require regular review to ensure they only contain those addresses of people who are still valid members of the group.

1.9 MIT gives no guarantee regarding the delivery of email or attachments or the accuracy of the data transferred once it is transmitted outside of MIT network.

1.10 Personal email notifications should be limited to reasonable and appropriate use.

2. Content

2.1 When sending email to multiple external recipients users must use the bcc field if there is an expectation that privacy is to be maintained. This ensures that the email addresses of all recipients are not disclosed to each other.

2.2 Users of the email system must ensure that information meant only for internal use is not sent to an external email address by error, by clicking ‘reply to all’ or by sending to a distribution list.

2.3 MIT restricts the size of incoming and outgoing emails and attachments to 25MB.

2.4 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 5.3 of the Acceptable Use Policy.

2.5 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 5.4 of the Acceptable Use Policy.

2.6 External email messages must have the approved MIT disclaimer attached so that the recipient of the information is aware of the limitations of use of the information provided, or any endorsements or qualifications that may apply.

This disclaimer will be automatically added to external emails by ICTS.

eMails may also be labeled with an approved labelling schema to highlight their sensitivity and value.

2.7 When the identity of the sender is not known the following applies:

- If the email is a simple request for information, then provide a response with the requested information or acknowledge receipt of the information as soon as possible e.g. What hours does your campus open?
- If the communication is more complex or contentious, then the sender should be asked to provide their name and address before a detailed reply is made.
- The recipient must in each case comply with all relevant legal requirements, including those set out in the MIT's Privacy Policy and Official Information Act Policy.

2.8 Users should not include any non-corporate background stationery, wallpaper or decoration on emails.

2.9 Users of the email system must not insert digital versions of written signatures so that it looks as though an email message was signed by the sender or someone else.

Furthermore, an approved email signature provided by Sales and Marketing must be used in all external email correspondence. This feature should be set in Exchange so that the signature is automatically added to outgoing email. Only mail being sent via the user's mobile device is exempt from this process as some devices don't support this feature.

3. Retention of eMail

3.1 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 5.5 of the Acceptable Use Policy.

3.2 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 5.6 of the Acceptable Use Policy.

4. Rights to Privacy

4.1 eMail messages will be continuously monitored for compliance with this Policy and for system management purposes. The email system should not be considered 'private' and authorised MIT staff may, at any time, view email files.

4.2 Users should presume that information sent by email is as visible as that written on a postcard. Unless the content is encrypted or protected by some other approved method, users may not send credit card information, PIN numbers, passwords and other sensitive information via email. This requirement also relates to documents sent as attachments.

4.3 The email system is the property of MIT and all messages sent or received by it, or stored within it, are owned by the MIT. MIT reserves the right to access and disclose all messages sent over its email system if required by law or valid business purpose providing permission has been granted by a Director.

4.4 MIT uses automatic email content scanning tools to identify selected keywords, file types, and other information and therefore it is recommended users restrict their communications to business matters. Messages that are deemed inappropriate will be blocked.

5. Incident Management

5.1 Any user who discovers a breach of the eMail Policy or email security is to notify the Head of ICTS or People & Culture immediately so that the correct remedial action can be taken.

5.2 Files received from an unknown, suspicious or untrustworthy source will be deleted immediately without opening. Under no circumstances should users click on links contained within an email message sent from an unknown source.

If the recipient has any suspicions about whether an email originates from an unknown, suspicious or untrustworthy source, advice should be sought from ICTS before opening the email or any attachments.

6. Spam Controls

6.1 Should users of the email system receive unwanted and unsolicited email (also known as spam), they must not reply to the sender. If spam is continuously received from a particular address users should notify the ICTS Service Desk who will block the address.

6.2 eMail, instant messages, text messages and tweets that are of a commercial nature and are being sent to external parties must comply with the requirements of anti-spam legislation. This requirement is particularly relevant to those using distribution lists.

Management Responsibilities

1. Restrictions of Use

1.1 Before a new user has access to the email system, a request to create a new user account (including user name, profile and email account) must be logged on MITDesk prior to the user starting. This request may need approval from the appropriate manager or People & Culture. All applicable information on the request form must be completed. Access is granted on the basis of a genuine need for this system to carry out day-to-day business activities on behalf of MIT.

2. Management of Users

2.1 Managers responsible for staff with email access must ensure that use is in accordance with MIT policies.

2.2 Managers are responsible for ensuring that staff comply with anti-spam requirements in accordance with anti-spam legislation. Managers must exercise a suitable level of control over bulk email depending on the individual needs.

Information, Communications and Technology Service Responsibilities

1. Retention of eMail

1.1 Emails, their attachments, archives and log files are subject to the same systematic document handling processes as any other corporate document and must be retained and disposed of as required by law and in accordance with the Records Management Policy and any applicable ICTS policies, guidelines and procedures.

1.2 MIT emails, attachments, archives and log files are legally owned by the MIT. They are considered evidential documents and must be disposed of in accordance with information management procedures.

If a legal suit or internal disciplinary hearing is pending they must be retained. Email is searchable and recoverable and a separate email archiving system has been implemented to meet this requirement.

2. Management of the eMail System

2.1 Anti-spam filtering is enabled and messages tagged as spam will be blocked.

2.2 Anti-virus is installed and operational on the email server and every email and attachment is scanned and quarantined if it contains any content that may be considered as potentially harmful.

2.3 Content filtering is enabled to ensure that any email or attachment containing unacceptable text, graphic or file is blocked.

2.4 Mail relaying is disabled on all devices connected both internally and externally to the network unless they are required for business purposes and approved by the Head of ICTS.

2.5 The system is configured to block all files with an extension that may potentially cause harm.

2.6 ICTS staff regularly monitor email traffic for high volumes which could indicate a denial of service situation, source address spoofing, spam generation or other system misuse with the potential to cause denial of service to legitimate users.

2.7 ICTS will only create user accounts that have been formally requested on MITDesk and approved by the relevant manager and People & Culture.

Access will be granted on the basis of a genuine need for this system to carry out day-to-day business activities on behalf of MIT.

2.8 The email archiving system will automatically remove emails that are older than 90 days from the inbox, sent and deleted folders. Once removed, these messages will only be accessible through Mail Archive.

2.9 When a staff member leaves MIT their email account is disabled.

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
eMail	Communication sent via MIT's electronic mail system.
MITDesk	MIT's service management system.
Outlook Web App (OWA)	MIT's email system delivered via the Internet.
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).