



## 1. INTRODUCTION

The purpose of this policy is to:

- I. Regulate access to Manukau Institute of Technology (“MIT”) Computer Systems ensuring they are used appropriately and effectively to support the business functions of the Institute and the delivery of high quality learning and teaching.
- II. Provide staff, students and other authorised users with clear direction regarding access to and appropriate use of MIT Computer Systems, and encourage their responsible use.

### *Scope*

This policy governs the use of MIT Computer Systems by all users including (but not being limited to) staff, students, and those who install, develop, maintain, administer and use those systems and its applications. This policy applies regardless of what technology tool is used to access MIT Computer Systems (including, but not limited, to desktop computers, laptops, Blackberry, PDA, or other handheld smart phone devices) or whether the system is accessed at MIT or offsite (including home).

## 2. POLICY

- 2.1. MIT will provide effective Computer Systems to support the business functions of the Institute and the delivery of high quality learning and teaching.
- 2.2. MIT will seek to ensure its Computer Systems are used efficiently and appropriately, and in a manner consistent with Institute policy, procedure and legal and statutory obligations, maintaining the highest ethical standards at all times.

## 3. PROCEDURES

- 3.1. The Director Finance and Infrastructure in conjunction with ICTS is responsible for ensuring:
  - I. MIT Computer Systems are available and maintained in order to effectively support the business functions and learning and teaching functions of the Institute.
  - II. The maintenance and administration of appropriate policies and regulations to support the effective and appropriate use of the MIT Computer Systems.
- 3.2. **Ownership**  
 Subject to any third party agreement, legal ownership of MIT Computer Systems belongs to MIT. All messages transmitted and received using the system; contact details and computer files stored on the system are assumed to be for the purpose of supporting the business goals of the Institute and are therefore considered Institute property unless ownership of intellectual property in them can otherwise be proved to belong to the user or other parties.

### 3.3. Authorised Access

**3.3.1.** In order to protect MIT and users of MIT Computer Systems, only authorised users may access the system.

**3.3.2. *Staff***

All requests for staff access to MIT Computer Systems must be made and approved by the Senior Manager or Director responsible for that staff member. Authorisation must be obtained by completing the online form found on MITNet under *Online Forms/New Staff Member* on the ICTS page.

**3.3.3. *Students***

Student access to MIT Computer Systems will be authorised by ICTS upon confirmation of a student's enrolment status with the Institute and their registration on Jasper (the MIT student management system). Once enrolled, student accounts are activated one week prior to the course start date.

**3.3.4. *Other authorised users***

In certain circumstances other persons may be granted access to MIT Computer Systems. All requests for such access must be made and approved by the Senior Manager or Director responsible. Authorisation must be obtained by completing the online form on MITNet.

**3.3.5.** Network and internet access extends throughout the term of a user's employment, contract, relationship or study at MIT providing they do not violate this policy.

***Termination***

**3.3.6.** Subject to section 3.3.8, access to MIT Computer Systems will be severed 3 weeks after the course end date or termination date of an MIT employment contract.

**3.3.7.** Upon termination of a staff member's access to MIT Computer Systems the following will occur:

***Emails***

- i. Access to the staff email account will be blocked and the email address *firstname.surname@manukau.ac.nz* will no longer be able to receive or send emails; and
- ii. The contents of the email account will be made available to the staff member's manager as a read only shared resource for a specified period of time after the staff member's termination of access as agreed between the manager and ICTS.

***Computer files***

- i. Home drive access will be locked and a copy restricted to the staff member's manager; and
- ii. Access to shared drives will be revoked. Where appropriate, a new group owner for the shared drives will be created

**Contact list**

- i. Access to the staff member's contact list on the system will be blocked;
- ii. A copy of the contact list will be provided to the staff member's manager.

- 3.3.8.** Should a staff member require continued access to MIT Computer Systems after the termination of their employment, a written exception must be authorised by the relevant Senior Manager or Director responsible for that staff member. Students requiring extended access must seek authorised access from the relevant Dean. It should be noted that upon termination of a student's study at MIT, the student MIT email account will be locked.
- 3.3.9.** Users may only access and use equipment, networks or information for which they hold specific authorisation.
- 3.3.10.** Users are responsible for the security of their passwords, accounts and data. Under no circumstances should a user disclose their password to a staff member, student, other individual or organisation unless required to do so by law (refer section 3.6.4).
- 3.3.11.** Users will be held responsible for the contents of their computer account and any transactions attributable to their User ID.

**3.4. Use of MIT Computer Systems**

- 3.4.1.** MIT Computer Systems are provided for business purposes to support the primary functions of the Institute and its administration. MIT Computer Systems (including Internet and email services) must only be used for:
- i. MIT business purposes.
  - ii. Student course of study.
  - iii. MIT research purposes.
  - iv. Reasonable personal use.
- 3.4.2.** MIT business purposes include any activity that is conducted for purposes of accomplishing MIT business related to research, learning and teaching, courses of study, administrative activities and professional development.

**Reasonable personal use**

- 3.4.3.** Reasonable personal use of MIT Computer Systems is permitted by users but must be limited to when the system is not required for its primary functions and for staff members only when it does not impede the work for which they are employed. As a guide, use that occurs more than a few times per day and/or for periods longer than a few minutes would not be considered reasonable personal use. This use should generally occur during personal time and **should not** include uses that:
- i. Require substantial expenditure of time.
  - ii. Are for private business, personal gain or profit.
  - iii. Involve participation in online gambling.
  - iv. Support political campaigns, candidates, legislation or ballot issues.
  - v. Impede the efficiency of intranet, internet or email services.

- v. Clog mailboxes with large numbers of messages (spam).
- vi. Waste MIT resources,
- vii. Would violate or breach any MIT policies, regulations or harm MIT's image or reputation.
- viii. Use valuable bandwidth.

***Statutory and ethical obligations***

**3.4.4.** Users must ensure their use of MIT Computer Systems is consistent with Institute policy, legal and statutory obligations (refer section 8) and maintains the highest ethical standards.

**3.4.5.** Without limitation, users must not use MIT Computer Systems (whether accessed at MIT or offsite including home):

- i. To access or try to access any part of any MIT Computer System to which that user is not authorised to access.
- ii. In breach of the requirements of the Privacy Act 1993.  
Resources are available on MITNet under *Staff Information/Privacy Principles Resources* to assist staff in the application of the Privacy Act 1993. Further assistance and guidance may also be sought from the Institute Privacy Officer (Legal and Contracts Team).
- iii. To engage in illegal activities including (but not limited to) accessing or sending:
  - a. Illegal, fraudulent or defamatory content and material.
  - b. Objectionable material.
  - c. Confidential information without appropriate authorisation.
  - d. Offensive, discriminatory or harassing material.
- iv. To distribute any material harmful to MIT or MIT's reputation or which may overload the MIT Computer System.
- v. To access inappropriate internet sites, including (but not limited to):
  - a. Sites that are illegal or hold illegal content.
  - b. Sites that contain pornographic or inappropriate sexual material.
  - c. Sites that advocate hate or violence.
  - d. Sites that offer games or software that are unrelated to academic programs.
- vi. To undermine or attempt to undermine network security or intentionally introduce, distribute or create viruses.
- vii. To take part in any dishonest activity including (but not limited) to cheating or plagiarism.
- viii. Misrepresent any personal view as being the views of MIT.
- ix. Enter into any legal agreement committing the Institute without the appropriate delegated authority (refer *Legal and Compliance Policy 1: Contractual Arrangements*).
- x. Read, delete, copy, modify or send any email message from another user's account without that user's permission.

- 3.4.6.** All electronic records created or maintained on the MIT Computer System must be stored, managed, maintained and disposed of (deleted) in accordance with the requirements of the Public Records Act 2005.  
Further information about the requirements of the Public Records Act 2005 is available from the MIT Records Manager.

***Internet and email services***

- 3.4.7.** A message sent to an MIT electronic mailing list must be relevant to the membership of that list.

***File Management***

- 3.4.8.** Users should save files/documents into their allocated home drive (H drive) or shared drive (Y drive) as appropriate. Users are advised that any files/documents saved on the desktop are not backed up and may be deleted permanently by ICTS.

***Respect for other users of MIT's Computer System***

- 3.4.9.** Successful use of the MIT Computer Systems depends upon the spirit of mutual respect and co-operation to ensure that everyone has equitable privileges, privacy and protection from interference or harassment.

- 3.4.10.** You must:

- i. Respect the privacy of other users and thus not intentionally seek information on, obtain copies of, or modify files, tapes, passwords or any type of data belonging to other users unless specifically authorised to do so.
- ii. Respect the integrity of the system and not use MIT resources to develop or execute programs that could infiltrate the system, tamper with or attempt to subvert security provisions, or damage or alter software components of the system.
- iii. Respect others by not listening to loud audio/music from the computer.

**3.5. Information Protection**

- 3.5.1.** Users should assume that communications made using the MIT Computer System may be read by someone other than the intended recipient. Content of a highly confidential or sensitive nature should be conveyed by another means. Email may be considered as being more like a postcard than a sealed letter.

**3.6. Monitoring and Privacy**

- 3.6.1.** Subject to any third party agreements, MIT Computer Systems are the property of MIT (refer section 3.2). Anything created, sent or received using the network; systems and facilities of MIT will therefore be transmitted and stored on MIT property.
- 3.6.2.** 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 may 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:
  - a) Identify inappropriate use.
  - b) Protect system security.
  - c) Maintain system performance.
  - d) Protect the rights and property of MIT.
  - e) Determine compliance with MIT policy.
- iii. Network traffic including:
  - a) Email and internet usage.
  - b) Usage data such as account names, source and destination accounts and sites.
  - c) Dates and times of transmission or access.
  - d) Size of transmitted material.
  - e) Other usage related data.

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

**3.6.4.** 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 process if there is litigation in progress (please refer to MITNet for relevant policies).

### **3.7. Connecting Devices to the MIT Network**

**3.7.1.** It is important to the Institute that the Computer System operates at optimum efficiency to ensure availability to all. Therefore other than MIT assets, no other device is to be connected (plugged in) to the MIT network without the express written permission of the network administrator (or an authorised delegate). Such permission may be obtained by the ICTS Manager.

**3.7.2.** Personal devices such as notebooks or smartphones may be connected to MIT's secure wireless network (MITwireless).

### **3.8. Copyright Compliance**

**3.8.1.** No material is to be used without the written permission of the copyright holder. It is illegal to place on a web page any pictures or videos of people without the permission of the people in the picture or video and/or the copyright owner.

**3.8.2.** MIT regards all of the software which it makes available to users as Proprietary Software. Software programs are protected by the Copyright Act. Users must not make and/or distribute copies of programs without specific permission of the ICTS Manager.

**3.8.3.** The MIT logos and designs are the property of MIT and may only be used on approved MIT documents.

<http://mitnet.manukau.ac.nz/ServiceCentre/ContractsLegal/trademark.asp>)

- 3.8.4.** The Institute Librarian or the Legal and Contracts Manager may be contacted for further guidance on copyright compliance.
- 3.8.5.** MIT will block Peer2Peer (P2P) file sharing software such as bittorrent, from accessing internet content to mitigate the risk of breaching the Copyright Amendment Act 2011. Any exception requests for allowing file sharing applications must be made to the Manager ICTS with appropriate justification.

### **3.9. Right of Review**

- 3.9.1.** These regulations are intended to ensure that use of any system for which MIT is responsible is ethical, legal and respectful of privacy, while at the same time protecting freedom of expression, particularly the exercise of academic freedom, at the Institute. This is both for the protection of individuals and for protection of the Institute and its reputation.
- 3.9.2.** If at any time a user feels their rights as a user are being violated, or become aware of other users who are misusing or abusing MIT Computer Systems, the problem should be reported promptly. In the first instance, such reports should be made to the user's immediate supervisor. Failing a satisfactory response a report should be made to the manager of the computer system you were using, or the user's Senior Manager, or to the Director of Finance and Infrastructure, in turn until a satisfactory response has been obtained.

### **3.10. Breach of Regulations**

- 3.10.1.** Any breach of these regulations shall be deemed to be a breach of the disciplinary regulations of MIT and in addition may lead to the user being temporarily or permanently refused access to the system.
- 3.10.2.** Any person aggrieved by such a refusal may apply in writing to the Chief Executive of MIT within 10 (ten) days of notice of such refusal.
- 3.10.3.** Should a person wish to appeal against the decision of the Chief Executive the appeal should be addressed to the Council of MIT within 10 (ten) days of notice of such refusal.

## **4. EVALUATION/OUTCOMES**

- 4.1.** Key performance indicators for MIT Computer Systems that support MIT Business functions and teaching and learning activity will be set and approved annually as part of the Institute strategic planning process.
- 4.2.** MIT Computer Systems supporting the delivery of learning and teaching will be the focus of SAEER and continuous improvement and will form part of the Institute's roster of reviews commissioned by the Academic Quality Assurance Sub-Committee of Academic Board (refer Academic Policy 8: Evaluation, Review and Monitoring).
- 4.3.** Using Institute SAEER processes, ICTS will evaluate and report annually to the March meeting of Academic Board on its performance supporting the delivery of learning and teaching activity and

against key performance indicators. This report will address issues encountered and measures taken for continuous improvement.

- 4.4.** MIT Computer Systems will be subject to MIT Service Centre Satisfaction surveys with outcomes used to inform the process of continuous improvement.

## 5. AUDIENCE

All staff, students and users of the MIT Computer System.

## 6. CONSULTATION SCOPE

Reasonable and appropriate consultation with staff and students. All users of MIT Computer Systems are to have access to this policy and must acknowledge the policy on login to the MIT network. The policy will be available on MITNet, Emit and the Institute website for staff and students to access and read.

## 7. RELEVANT DELEGATIONS

**7.1.** Pursuant to Section 196 of the Education Act 1989, the Chief Executive is responsible for the management of the academic and administrative affairs Institute.

**7.2.** Chief Executive to the Director of Finance and Infrastructure (delegation): authority to manage the operation of the MIT Computer Systems in conjunction with ICTS.

**7.3.** Chief Executive to Senior Managers and Directors (authorisation): authority to approve authorised users of the MIT Computer Systems in accordance with provisions of this policy.

### *Evaluation*

**7.4.** Council delegation to the Academic Board: Authority for the monitoring and application of quality assurance requirements with respect to supporting learning and teaching through quality evaluation, review and reporting processes (Statute 5 Register of Delegations AB TBA).

## 8. RELEVANT LEGISLATION

Copyright Act 1994  
Crimes Amendment Act 2003  
Electronic Communication Act 2005  
Equal Opportunity (Employment Relations Act 2000)  
Films, Videos and Publications Classification Act 1993  
Harassment Act 1997  
Human Rights Act 1993  
Official Information Act 1982  
Privacy Act 1993  
Public Records Act 2005

## 9. LEGAL COMPLIANCE

This policy complies with Institute statutes, regulations and relevant legislation.

## 10. RELATED DOCUMENTS AND FORMS

Terms and conditions for using MIT Computer Systems.  
Catalogue of Services  
Student MIT Computing Quick Start Guide

## 11. DEFINITIONS

**“Chief Executive”** means the person appointed by Council to the Office of Chief Executive of MIT pursuant to section 180 (a) of the Education Act 1989.

**“Council”** means the governing body of MIT constituted in accordance with Part 15 of the Education Act 1989.

**“Computer Systems”** means any computer or computer system controlled and/or operated by MIT including, but not limited, to desktop computers, laptops, Blackberry, PDA, or other handheld smart phone devices and the applications, software, internet, email, network accessed via these systems, and the storage of information on these systems.

**“Director”** means a member of the Leadership Team and for the purposes of this policy includes the Chief Executive.

**“ICTS”** means MIT Information and Communication Technology Services.

**“ICTS Manager”** means the Information and Communication Technology Services Manager. The person or persons authorised by the Chief Executive to control the Institute computer systems.

**“Institute”** means the Manukau Institute of Technology.

**“MIT”** means Manukau Institute of Technology.

**“Network device”** means network devices which are components used to connect computers or other electronic devices together so that they can share files or resource, like laptops (other than wireless internet connectivity), printers and fax machines.

**“SAEER”** means the process of Self Assessment and External Evaluation and Review administered by NZQA which forms the quality assurance framework for New Zealand tertiary education providers (other than Universities) focusing on the quality and value of the outcomes achieved in tertiary education and the key processes that contribute to them.

**“Senior Manager”** includes Deans, Heads of Department and Managers of service centres.

**“Staff”** means a person under an employment contract at the Institute on a full-time, part-time, or casual basis and for a permanent or fixed-term duration.

**“Student”** means a person currently enrolled on a programme at the Institute.

**“Users”** means the persons authorised to use the MIT Computer Systems. Any person not so authorised shall not use any system.

**“User ID”** means the unique user identifier which identifies a person to the computer network.

## 12. DOCUMENT MANAGEMENT AND CONTROL

<b>Category</b>	Management – Information Technology
<b>Sponsoring Director</b>	Director Finance and Infrastructure
<b>CE Approval Date</b>	28 <sup>th</sup> April 2010
<b>Council Minute</b>	NA
<b>Academic Board Minute</b>	NA
<b>Effective Date</b>	28 <sup>th</sup> April 2010
<b>Review Date</b>	April 2012
<b>Version</b>	1