

STAFF COMPUTER USE

Section	Human Resources		
Approval Date	18.05.09	Approved by	Directorate
Next Review	As required	Responsibility	Director of Finance and Corporate Services
Key Evaluation Question	6	ITPNZ Quality Standard	3

PURPOSE

To ensure that the Institute's computer network is protected from misuse and damage.

To clarify and minimise potential liability for the Institute and staff in using e-mail and the Internet.

SCOPE

All staff and contractors with access to NMIT's computer network.

Any computer systems, devices or infrastructure owned by NMIT.

All material contained in an electronic message, sent or received internally or externally, including attached documents and files.

COMPUTER USE

NMIT computer services and systems are provided to assist staff with their work.

NMIT will not accept liability arising from personal use of the Institute's computer or e-mail systems. The Institute's computer systems or e-mail may not be used for personal financial gain or for private business purposes.

Reasonable personal use of the internet is permitted but should be kept to minimum, should not interfere with staff work responsibilities or encroach on staff working hours.

Accessing or using offensive, obscene, discriminatory, pornographic or otherwise inappropriate material through the internet or on the computer system may result in disciplinary action.

E-mail travels via the Internet which is an insecure medium. Staff should exercise discretion in the content as e-mail messages may be accessed by users other than the intended recipients. Do not use e-mail for confidential information.

E-mail messages sent or received using the Institute's facilities are not private; they are the Institute's property. Nelson Marlborough Institute of Technology reserves the right to monitor, access and to disclose e-mail messages.

E-mail messages are frequently saved or printed and retained as business records and should be appropriately worded.

False statements in an e-mail message about a person or organisation, which makes a claim, expressly stated or implied to be factual, that may give an individual, business, product, group, government or nation a negative image, can amount to defamation. Consider the privacy principles relating to protection and disclosure of personal information.

Staff should exercise discretion in sending private messages (eg advertising) to staff and be aware that disruption may occur through the misuse of mailing lists, wide distribution without good purpose or flooding an individual, group or system with numerous or large e-mail messages. Consider using the established line management communication channels rather than sending e-mails to 'all staff' as a first option.

Inappropriate use of e-mail can constitute harassment and result in disciplinary action. Refer: *Harassment Act 1997; Staff Misconduct Procedure*.

Almost every country has copyright laws and staff must observe copyright requirements when using material from the Internet or made public on the computer network. Cite all quotations, references and sources.

Staff should regularly delete unnecessary files and folders. The Institute reserves the right to restrict access to computer services for staff using excessive network space.

SECURITY

All staff are responsible to ensure that the intellectual and physical assets of the Institute are protected by adopting accepted computer security practices, and personally accountable for the security of activities and files under their login account

All staff should:

- Select a "strong" (difficult to guess) password and keep it secure (do not share, write down or store passwords online).

Passwords should :

- Have a minimum of 7 characters
 - Contain 3 of the following – Lowercase, Uppercase, Digits, Punctuation, and Special character
 - Be changed regularly, and
 - Be easily remembered, but difficult to guess.
- Report any security breach (or potential breach) to IT Services, - or suspected unauthorised access to confidential information..
 - Not knowingly introduce a virus to the NMIT network
 - Ensure computers are secure, particularly when logged on, and that access to data is kept secure when computers are left unattended by locking their workstation.
 - Ensure that the Institute computer security systems are supported and not overridden.
 - Ensure that hardware or software is not added, removed or modified without prior authorisation.
 - Only connect devices authorised by IT Services to the NMIT network.

- Regularly check drives such as USB/Pen drives for virus contaminants via the Helpdesk.

REFERENCES

INTERNAL

Staff Misconduct Procedure
Preventing Harassment
External Communications and the Media
Copyright, Explanation for Staff

EXTERNAL

Human Rights Act, 1993
Privacy Act, 1993
Harassment Act 1997