# Use of Information Technology

## Overview

As part of Nelson Marlborough Health's commitment to the productive use of information technologies, many employees use computers and other devices such as smartphones, which gives access to email and the internet.

## Purpose

The purpose of this policy is to provide rules and guidelines for the acceptable use of Nelson Marlborough Health computing and communication resources, including computers, networks, electronic mail (e-mail) services, electronic information sources, and other communication resources.

## Scope

All Nelson Marlborough District Health Board employees and contracted staff with access to computers and mobile devices must follow this policy.

## Exemptions

In certain cases the General Manager IT may grant exemptions to this policy such as approving the use of Generic Logons.

## Definitions

Information technologies, devices, and NMH Infrastructure include:

- Computers
- Landline telephones
- Data cards
- Networks, including internet connections
- Cloud Services (eg Dropbox, Slack)
- Cellphones
- Smart Phones
- Memory sticks
- External hard drives
- Servers
- Email and internet
- Tablets

## Access

NMH must protect both the physical and information assets it owns. To ensure this:

- Only authorised people may gain access to NMH's server room facilities
- Only authorised people may gain access to NMH's network
- Users must attend appropriate training prior to gaining access to NMH applications
- Users may not alter any system settings on any NMH device or software installation.
- Users may change user level settings such as "flight mode".
- Creation of access accounts requires the authorisation of the area's manager, and the application administrator for each NMH application.

## Security

NMH must protect the privacy of the information it holds. To ensure this:

- Generic logons will not be used to access applications without approval of the General Manager IT.
- Audit capabilities will be available for clinical applications.
- User IDs/passwords must not be shared, written down, or stored electronically. e.g. do not save the network account password in the browser (if prompted).
- Accounts will be disabled upon a relationship with NMH ceasing.
- Users are accountable for the security of any information in their possession, including on portable storage devices.
- Users are encouraged to lock their workstations when they are left unattended by holding down the "Windows" key and the letter "L" simultaneously.

## Connection to the NMH infrastructure

To help prevent the spread of malicious applications, optimise support costs and maintain preferred supplier relationships, NMH must control the devices that are connected to the Board's infrastructure. To ensure this, **only equipment authorised by NMH may be connected to the NMH infrastructure.**

## Changes to the NMH infrastructure

NMH must manage infrastructure changes to ensure that risks to the infrastructure and application environment are minimised.

- All such change must follow NMH's Change Management Guidelines.
- Users may not alter any system settings on any NMH device.

## Remote Access

Remote access to NMH's application and infrastructure carries certain risks that need to be managed.

NMH's ICT engineers will provide the necessary connectivity and the appropriate security requirements.

All remote access must be approved by an appropriate NMH manager and the ICT Manager.

## Portable Storage Devices

All portable devices, including USB storage devices (USB keys, memory sticks), external hard drives and unapproved cloud services and are not recommended for use within NMH. If such devices are used, users must be aware that they are not backed up by NMH. They must be kept physically secure at all times and must not store patient identifiable information. Smart phones are another source of storage and must be locked by a secure PIN.

## Appropriate use of NMH information technologies

Employees should be aware that use of NMH information technologies is monitored, logged and audited by the organisation to ensure compliance with this policy. Use of applications, email, internet and mobile devices is recorded and traceable to individual users.

Employees are expected to use NMH information technologies appropriately, responsibly and not to breach any legislation or other NMH policies, nor to use such technology to perform any illegal activities.

Refer to the conditions applying to specific technologies below.

## Inappropriate use of NMH information technologies

NMH users must not engage in any activity that could be reasonably construed as offensive or abusive to other persons or the Board.

NMH information technologies may not be used for purposes including, but not limited to: pornography, copyright infringement, obscenity, slander, libel, fraud, defamation, plagiarism, forgery, impersonation, gambling, soliciting for illegal pyramid schemes, wilful tampering (e.g. spreading computer viruses), privacy infringement (e.g. the unconsented use of camera phones) or harassment, intimidation or abuse (e.g. text bullying).

## Consequences of inappropriate use

Breach of the rules and conditions described in this policy shall be investigated and may be subject to the provisions of the NMH *Disciplinary Code*.

## Conditions of email use

Emails containing file attachments less than 50 megabytes will be delivered/sent. Any files greater than 50 megabytes will be rejected and the sender notified that the message/attachment has been rejected as a result of the file attachment restrictions.

Users must not join personal mailing lists using their NMH email address. Such mailing lists generate a large volume of email to NMH.

"All User" emails may only be sent by staff with the delegated authority to do so.

Users must not auto-forward NMH emails to private email addresses.

Staff must take precautions against introducing viruses into the computer system such as not opening files or attachments from unknown parties. Where a staff member suspects a virus may have been introduced to NMH computer systems they must advise the Help Desk immediately.

NMH does not guarantee the delivery of any email.

## Professional standards

NMH, as a government-funded health service organisation, requires a high standard of professionalism in its communications, which may be above that of other organisations.

Email communications sent from NMH travel on our "electronic stationery" and employees should treat them in the same manner as if the communication were sent on letterhead paper.

Professionalism should be maintained in all email communications and this should be reflected in the language, content and grammar used.

Email users should be aware that internal messages between NMH employees, as well as external emails, are "discoverable" under the Official Information Act

## Privacy of information in emails or on the internet

Emails need to comply with Clinical Governance Guidelines and all DHB privacy policies. The internet is not a secure medium for exchanging information. Sensitive material transferred over the internet may be at risk of detection by a third party. Email messages can easily be copied and forwarded on to other people without the original sender's knowledge or approval. Employees must exercise caution and care when transferring sensitive material in this form.

Where an internal email has patient-identifiable information, the sender should ensure that the intended recipient is entitled to receive such information. External internet email is not a secure medium so patient-identifiable information must not be emailed to recipients outside of NMH unless the patient has provided consent to do so.

## Conditions of internet access

Users may not install applications from the internet and minimise applications that require an internet connection (e.g. Google Earth, iTunes).

Users may not access internet content that generates large amounts of traffic, such as streaming audio and video, which are not directly related to NMH operations.

Employees shall not place company material (copyrighted software, internal correspondence, etc.) on the internet without prior permission.

Users must not attempt to interfere with NMH's internet and security settings.

## Personal use - email and internet

Personal use of NMH communication technologies, subject to the conditions stated above is permitted if it does not interfere with work responsibilities.

Personal use of email, the internet or mobile devices must not compromise or interfere with the performance or use of these systems by staff for work purposes.

Messages sent via NMH email remain the property of the NMH and may be accessed by the organisation at any time. Email communications should, therefore, be considered as non-confidential.

The delivery of personal internet email to and from NMH users is not guaranteed.

NMH may limit access to internet sites that are not related to NMH's business. Such restrictions may be for security, content or traffic management reasons, e.g. www.trademe.co.nz.

## Conditions of mobile device use

NMH will fund:

- Business-related mobile device expenses.
- Restricted International roaming costs, when the travel relates to NMH operations.

NMH will not fund:

- Expenses relating to games, ringtones, wallpaper, weather, news reports, picture messaging, video, 0900 services or similar.
- Unauthorised International Roaming costs.

## Guidelines for mobile device use

NMH calling plans for 2Degrees cell/smart phones provides unlimited calling and texting to New Zealand and Australian landlines and cellphones. All calls from NMH landlines to 2Degrees cell/smart phones are also free.

All data use is restricted to business related purposes only.

## A greener NMH

Computers contribute to NMH's power consumption. When not in use for extended periods, including overnight, personal and laptop computers should be turned off, unless a specific request is made by ICT.

## Associated documents

NMH Disciplinary Policy

NMH Change Management Guidelines

NMH Code of Conduct

## User Statement

Every person employed by or contracted to NMH and authorised to use NMH information technology including email, internet, and mobile devices must sign and date a statement that they have read and understood the terms and conditions of this policy and its contents, that they will comply with the policy at all times, and acknowledge that NMH reserves the right to monitor any communication sent or received through the DHB's technology infrastructure.

# User Statement

In consideration of receiving access to *NMH's email / internet / mobile devices* I confirm that I have read and understood the NMH *Use Of Information Technology* policy and will comply with the policy at all times.

I acknowledge that any breach of the *Use Of Information Technology* policy may lead to disciplinary action.

Signed: _____ Dated: _____/_____/_____

Print Name: _____ Log-On ID: _____

Manager Name: _____