POLICY USE OF INFORMATION TECHNOLOGY

Overview

As part of Nelson Marlborough District Health Board's commitment to the productive use of information technologies, many employees use computers, giving access to email and the internet, mobile telephones and other mobile devices such as PDAs and laptop data cards.

Purpose

The purpose of this policy is to provide rules and guidelines for the use of current and new communication and information technologies.

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, Corporate Services, may grant exemptions to this policy.

Policy statement

Nelson Marlborough District Health Board (NMDHB) encourages and supports the use of information technologies to facilitate business communications within and outside the organisation. NMDHB provides such technologies to staff to enable them to carry out NMDHB business more efficiently.

Definition

Information technologies and devices – NMDHB Infrastructure

These include:

- computers
- mobile telephones
- data cards
- iPods
- networks, including internet connections
- email and internet
- personal digital assistants (PDAs)
- memory sticks
- external hard drives
- servers

Access

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

- only authorised people may gain access to NMDHB's server room facilities
- only authorised people may gain access to NMDHB's network
- users must attend appropriate training prior to gaining access to NMDHB applications
- users may not alter any system settings on any NMDHB device or software installation
- creation of access accounts requires the authorisation of the area's manager, and the application administrator for each NMDHB application.

Security

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

- generic logons will **not** be used to access applications
- clinical applications will record a log of all transactions
- user IDs/passwords must not be shared, written down, or stored electronically
- accounts will be disabled upon a relationship with NMDHB ceasing
- users are accountable for the security of any information in their possession, including on portable storage devices.

Connection to the NMDHB infrastructure

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

Changes to the NMDHB infrastructure

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

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

Development

NMDHB needs to ensure software developed by NMDHB, or by third parties specifically for NMDHB can be supported into the future.

- Development work must follow NMDHB's *Development Guidelines.*
- All source code and associated artefacts must be placed in the NMDHB source control system.

Remote access

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

- Remote access to NMDHB must follow NMDHB's *Remote Access Guidelines.*

Portable storage devices

Portable devices, including iPods, USB storage devices (USB keys, memory sticks), and external hard drives are not recommended for use within NMDHB.

If such devices are used, users must be aware that they are not backed up by NMDHB, and must be kept physically secure if they hold patient-identifiable information.

Appropriate use of NMDHB information technologies

Employees should be aware that use of NMDHB 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 NMDHB information technologies appropriately, responsibly and not to breach any legislation or other NMDHB policies, nor to use such technology to perform any illegal activities.

Refer to the conditions applying to specific technologies below.

Inappropriate use of NMDHB information technologies

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

NMDHB 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 NMDHB *Disciplinary Code.*

Conditions of **email use**

- Emails containing movie files, sound files, executables files or large attachments of a personal nature will be deleted and not delivered.
- Users must not join personal mailing lists using their NMDHB email address. Such mailing lists generate a large volume of email to NMDHB.
- "All User" emails may only be sent by staff with the delegated authority to do so.
- 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 NMDHB computer systems they must advise the Help Desk immediately.
- NMDHB does not guarantee the delivery of any email.

Professional standards

- NMDHB, 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 NMDHB 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 messages between NMDHB employees which criticise other individuals or organisations are "discoverable" under the Official Information Act and could be used in any defamation case brought against the NMDHB. Such criticism should therefore be avoided.

Reliability and privacy of information in emails or on the internet

- The truth or accuracy of information on the internet and in email should be considered suspect until confirmed by a separate (reliable) source.
- Use of the internet or email does not guarantee the privacy or confidentiality of information sent or received. 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 NMDHB.**

Conditions of **internet access**

- Users may not install applications from the internet or use non-NMDHB applications that require an internet connection (e.g. Skype, Google Earth, iTunes).
- Users may not access internet content that generates large amounts of traffic, such as streaming audio and video, which are not related to NMDHB 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 NMDHB's internet and security settings.

Personal use - email and internet

- Personal use of NMDHB communication technologies, subject to the conditions stated above, is permitted provided that 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 NMDHB email remain the property of the NMDHB 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 NMDHB users is not guaranteed.
- NMDHB may limit access to internet sites that are not related to NMDHB's business. Such restrictions may be for security, content or traffic management reasons, e.g. *www.trademe.co.nz*.

Conditions of **mobile device use**

NMDHB will fund:

- business-related mobile device expenses
- roaming costs, when the travel relates to NMDHB operations. This must be pre-approved by a manager with delegated authority
- limited personal calls whilst staff members are on travel relating to NMDHB business.

NMDHB will not fund:

- expenses relating to games, ringtones, wallpaper, weather, news reports, picture messaging, video, 0900 services or similar
- roaming costs for personal calls.

Guidelines for mobile device use

- Calls to and from mobile phones are more expensive than landline usage. The exception is calling NMDHB mobile phones or landlines from a NMDHB mobile phone on a monthly plan - these are free
- Roaming costs are extremely high, and charges are made for both incoming and outgoing calls. Users should contact the telephone operators for alternative arrangements, such as loan phones from the country of travel.

Personal use - mobile devices

- Personal usage of mobile devices is permitted; however, users must set up a dual billing system via the telephone operators. This facility allows calls made with a prefix of ## to be billed directly to the employee. NMDHB's rates are charged.
- Personal calls must be made with the prefix ## to enable personal billing.

A greener NMDHB

Computers contribute to NMDHB's power consumption.

When not in use for extended periods, including overnight, personal and laptops computers should be turned off, unless a specific request is made by the Infrastructure CIO Group.

Associated documents

NMDHB *Disciplinary* policy

NMDHB Guidelines:

- *Change Management*
- *Remote Access*
- *Development*

User Statement	Every person employed by or contracted to NMDHB and given access to email, internet or the use of a mobile phone 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 NMDHB reserves the right to monitor any communication sent or received through the DHB's technology infrastructure. See *User Statement* below.

Important Note

This sign-off form is intended for new and current staff who are authorised by their manager to have internet access. Some people that sign this may not necessarily be entitled to internet access. The manager must tick the Internet Access box on the New Appointment IT form to authorise the access. For current staff to have internet access the manager must also fill out and sign a New Appointment IT form with the Internet Access ticked. Both situations must follow these guide lines and ensure the User Statement below is completed.

User Statement

In consideration of receiving access to *NMDHB's email / internet / mobile devices* I confirm that I have read and understood the NMDHB *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: _____________________________