

# POLICY

## INTERNET - ACCEPTABLE USE

Applicable to: **MidCentral DHB**  
**Including MidCentral Health & Enable NZ**

Issued by: **Information Systems**

Contact: **Manager Service Delivery**

### 1. PURPOSE

This policy establishes the acceptable use of the Internet by MidCentral District Health Board staff using MidCentral District Health Board systems. The purpose of this policy is to minimise the costs and risks incurred by MidCentral District Health Board through the provision of clear guidelines and standards for the use of the Internet.

### 2. SCOPE

All employees of MidCentral District Health Board and its subsidiaries and all contractors who are provided with a MidCentral account for internet usage.

Enable NZ has its own Information technology department and the following role translations apply:

- Information Systems Manager - Information Technology (Enable NZ)
- Security Officer – Information Technology Manager (Enable NZ)
- Information Systems - IT team (Enable NZ)
- Servicedesk – Trackit Helpdesk (Enable NZ)

### 3. DEFINITIONS

<b>MidCentral District Health Board</b>	Refers to the New Zealand Public Health sector entity known as MidCentral District Health Board and all of its subsidiary organisations e.g. MidCentral Health and Enable NZ.
<b>Business Use</b>	Internet information sought in conjunction with MidCentral District Health Board business activities.
<b>User Logins</b>	User logins are the individual logins assigned to users. These are generally unique to a user, and must not be shared with other users.
<b>Personal Use</b>	Use for purposes other than the business activities of MidCentral District Health Board e.g. use of the Internet to research topics not related to the business activities of MidCentral District Health Board.
<b>Internet</b>	Access to and use of the global electronic communications network and its supporting framework, commonly known as the World Wide Web which is external to the private networks owned and operated by MidCentral District Health Board.
<b>Computer system</b>	Describes the totality of a computer and including but not limited to local, remote, or removable storage devices or media.

### 4. ROLES AND RESPONSIBILITIES

#### **Information Systems**

Information Systems will provide Internet access to all employees and contractors.

#### **All Employees**

All employees and contractors will be personally responsible for their own actions in the use of the internet and to ensure that these guidelines are followed.

### 5. POLICY

- MDHB
  - Encourages the use of Internet access to share appropriate information and to improve communication; and
  - Prohibits unauthorised, unacceptable and improper use of this means of communication.
  
- Any Internet account associated with MDHB or assigned by MDHB to individuals, groups or particular functions is the property of MDHB.
  
- MDHB may wholly or partially restrict a users internet access without prior notice in the following circumstances:
  - When required by law
  - When breaches of this policy and/or the law have taken place
  - On the direction of the Chief Executive, Manager Service Delivery or delegate

Those who use the MDHB Internet access are expected to do so responsibly. They must comply with all legal requirements, with this policy, and other relevant policies and procedures.

- All users must have signed a [Declaration of Confidentiality](#) (See MDHB-1943) before being issued with internet access.
- It is essential that users accessing the internet are able to be clearly identified as an individual. Accordingly only individual internet accounts will be issued and NOT generic group accounts.
- Interpretation as to what is acceptable Internet usage is the responsibility of the Information System Manager Service Delivery.

### **Responsibilities**

- Use of Internet services must not compromise the professional integrity and duties, or the style and quality of the MDHB communications.

### **Prohibited**

The following use of the Internet is prohibited:

- Obtaining, producing or distributing material which is considered "offensive material" "harassing" "threatening" or "objectionable" under the following Acts:
  - Films, Videos and Publications Classification Act of 1993.
  - Human Rights Act 1993 or the Employment Relations Act 2000.
  - Unsolicited Electronic Messages Act 2007
  - Human Rights Act 1993 or the Employment Relations Act 2000.
- Accessing, sending, receiving or soliciting sexually explicit messages or images.
- Downloading or sending of any copyright protected materials in contravention of that copyright.
- Sending, receiving or down-loading any computer file which is deemed to be incompatible with the business of MDHB or which may present a risk in terms of computer operations: Such files include but are not limited to:
  - Streaming Video or Audio services
  - Movies e.g. file extensions avi, mov, mpeg, vivo
  - Music e.g. file extensions mp3, wav
  - Executable files e.g. file extensions exe, com
  - Databases e.g. file extensions mdb
  - VB Script e.g. file extensions vbs
  - Games
- Sending unsolicited "junk" mail, "for profit" messages or sending or participating in chain letters, pyramid schemes or other illegal schemes. E-mail messages containing warnings regarding viruses or other 'helpful' tips should be validated with Information Systems ServiceDesk before being forwarded.
- Interference with employment duties, or other obligations to the Board.
- Illegal, fraudulent or unlawful activity.
- Incitement to break the law.

- Misrepresentation of MidCentral District Health Board or communications that bring it into disrepute.

### **Privacy**

- There is no right of privacy with Internet usage for the user of a MDHB account. MDHB is not obliged to, but reserves the right to monitor and access all aspects of employees' internet usage at any time for any reason without prior notice to the employee.

### **Recording and Monitoring**

- MDHB uses an Internet gateway sentry system in conjunction with a filtering list. This records a complete audit trail by user of all websites visited, bandwidth used, the length of time spent at sites and the amount of data transferred. Access to sites that are classified under specific topics deemed unacceptable by MDHB, will be blocked. Internet users will be advised through their browser session when access to a website has been blocked. If a valid business related website has been inadvertently blocked the user should contact the Information Systems ServiceDesk.

### **Disclosure**

- Internet activity on systems maintained by the MDHB, may be considered to constitute a Board record and be subject to disclosure under law, or as a result of litigation.

### **Personal Use of the Internet**

- Limited personal use of the internet is acceptable to the extent that it does not have a detrimental effect on an employee's performance of their duties and does not interfere with or compromise the performance or use of the system for business related purposes.

### **Ownership**

- All computer systems owned by MDHB including but not limited to the internet access system, PC hard drives, server hard drives, and all data and information stored on them is the property of MDHB.
- MDHB reserves the right to use all information on its system for such purpose as it sees fit at any time for any reason without notice to the user. Such use is only restricted by prevailing New Zealand law and statute.

### **Audit Access**

- An examination of a randomly selected number of computer systems including but not limited to Internet files, may periodically be carried out by Information Systems or in response to a request from the Chief Executive or from the Manager responsible for the computer system in question.
- MDHB may at any time open and examine the contents of any data or other file held on a internet connected computer system. Audits of Internet access may include key words or phrases, sites visited, the length of time spent at sites and overall and the amount of data transferred.
- Audits and investigations of misused Internet Access will be carried out with due diligence and respect for employees. This includes adherence to any and all applicable provisions of the Privacy Act 1993 and the Human Rights Act 1993.

- Where audits show minor breaches of the policy for Internet access, the Manager Service Delivery will bring it to the attention of the individual user. For more serious or repeated breaches of the policy, the evidence of such breaches will be passed immediately to the employee's manager. Access to Internet services by the employee may be suspended pending the outcome of subsequent investigations. The employee's manager will advise the user and provide to them a copy of the evidence of abuse.
- The employee's manager and the HR manager (or their appointed deputies) will determine any further action to be taken. Such action will be in accordance with the MDHB Disciplinary Code.

### **Consequences**

Contravention or circumvention of this policy may constitute Misconduct or Serious Misconduct under the MidCentral District Health Board Code of Conduct and House Rules and may result in disciplinary action which may include dismissal.

## **6. RELATED MDHB DOCUMENTS**

MDHB-1943	Information Technology Systems Security and Access -Policy-
MDHB-5367	Mobile Computing, Portable Storage Devices and Wireless Acceptable Use
	-Policy-
MDHB-5365	E-Mail -Policy-

## **7. KEYWORDS**

Information Systems, Internet, Internet acceptable use, Web, WWW