E-mail, Internet, and Computer Policy (District)

This policy outlines the responsibilities and requirements of users of computing and communications resources of Southern District Health Board.

Policy Applies to

All employees of Southern District Health Board (Southern DHB), including temporary employees and contractors, must comply with this policy. It also applies to any person who is involved in the operation of Southern DHB, including joint appointments, volunteers, those with honorary or unpaid staff status and prospective employees applying for employment.

Policy Summary

This policy defines the boundaries of acceptable use of Southern DHB computing and communication resources, including computers, networks, electronic mail (e-mail) services, electronic information sources, and other communication resources.

Introduction

Users of Southern DHB's computing and communications resources are required to comply with this policy, other applicable Southern DHB policies, and related New Zealand legislation.

If a prospective user is uncertain about usage or policy (including any part of this policy), he or she must query his or her manager or Information Systems (IS) for clarification **before** use.

Resources

Southern DHB's computing and communication resources remain the property of the DHB at all times. They are to be used in accordance with Southern DHB policy and best practice guidelines. When a user's association with the DHB ends, it will terminate access to computing and communications resources and accounts.

Requirements for Use of Southern DHB Computing and Communications Resources

General

Users must comply with Southern DHB policies, and with all related New Zealand laws and regulations (see references below).

Note: ALL records, including clinical and corporate, are subject to the Public Records Act 2005. In order to assist Southern DHB to maximise the benefit from provisions under the Act, Archives NZ has developed a General Disposal Authority especially for District Health Boards: See Retention Schedule - General Disposal Authority for District Health Boards - which all Southern DHB employees must comply with, particularly in relation to the

minimum retention period stated and disposal action for each individual record.

Users must respect the rights and privacy of others, including intellectual property and personal privacy rights. (However, as the owner of the system and equipment, Southern DHB has the right to review information stored or sent. If there is a basis to do so this will be reviewed from time to time.)

Users must not compromise the integrity of the electronic network, and must refrain from activities that may damage either the network, or transmitted or stored data.

Personal

Users must be honest and accurate in personal and computer identification.

They must use their own computer log-on identifications (IDs). It is the individual's responsibility prior to using a device to log out of any active session that is not logged on using his or her ID.

Users must maintain the security of their own accounts. They are advised to protect their account passwords and to change them regularly.

Limited, occasional and brief private use of Southern DHB's computers, e-mail and internet systems are acceptable as long as it does not affect your work, the work of others, or the reputation of Southern DHB. Refer to the Code of Conduct and Integrity (Regional) (18679).

Note: Personal use **excludes** websites such as Trade Me, Sella, You Tube, Facebook, etc. These websites can be accessed from the in-house cafés in both Otago and Southland. This is a Southern DHB Board directive.

Personal Data Storage Devices

Use of private storage devices to hold conference, presentation, and/or work-related information, is permitted with caution. This includes, but is not limited to USB memory sticks, CDs, DVDs, and flash cards. The user must scan the storage device with DHB anti-virus software before opening any files using DHB computers.

Note: Users unsure how to scan a device should contact the Service Desk, extn 9888 or 03 470 9888.

Prohibited Uses of Southern DHB Computing and Communications Resources

The following uses or misuses of Southern DHB computing and communications resources are expressly prohibited.

General

- Use of DHB computer resources or electronic information without authorisation or beyond one's level of authorisation.
- Altering or attempting to alter files or

systems without authorisation.

- Altering or attempting to alter any DHB computing or networking components, including but not limited to computers, routers, switches, and hubs.

- Use of private computer hardware on the DHB network, including but not limited to, laptops, desktop computers, personal digital assistants (PDAs), and projectors without written approval from IS and the user's appropriate manager.

Note: Such equipment can be supplied by IS.

- Failure to comply with requests from a line manager to discontinue activities that might threaten the operation or integrity of computers, systems, or networks, or **otherwise violate this policy,** may result in loss of computing privileges and/or disciplinary action.

Security

- Intentionally or recklessly compromising the privacy or security of electronic information.

- Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorisation.

- Making DHB computing resources available to individuals not affiliated with Southern DHB without approval of an appropriate management authority.

- Unauthorised scanning of networks for security vulnerabilities.

Commercial

- Use of DHB computer resources for private business or commercial activities, or for fund-raising or advertising on behalf of non-DHB organisations. Unless appropriate, authorisation is sought and received to do so.

- Unauthorised reselling of DHB computer resources.

- Infringing upon the copyright, trademark, patent, or other intellectual property rights of others with respect to computer programmes or electronic information (this includes plagiarism).

- Unauthorised storing, copying, use, or reproduction of audio files, images, graphics, computer software, and other protected property, except as permitted by law.

Dishonesty

- Misrepresenting or forging the identity of the sender or the source of an electronic communication.

- Altering the content of a message originating

	from another person or computer with intent to deceive. ▪ Unauthorised attempts to acquire and use the passwords of others. ▪ Unauthorised use of, and attempts to use, the computer accounts of others. ▪ Interception or attempted interception of communications by users not authorised or intended to receive them. **Note**: Users who simply receive a message in error should notify the sender immediately and delete the message.
Malice and Negligence	▪ Unlawful communications, including but not limited to harassment, threats of violence, obscenity and objectionable material/pornography. ▪ Accessing, transmitting, storing or downloading any form of pornographic, sexually explicit, or inappropriate material. ▪ Unauthorised modification, or deletion, of another person's files, account, or newsgroup postings. ▪ Interference with, or disruption of, the computer or network accounts, services, or equipment of others. ▪ The intentional transmission of computer 'worms' and 'viruses', sending of electronic chain mail, 'denial of service' attacks, and inappropriate broadcasting of messages to large numbers of individuals or hosts. ▪ Negligent or intentional conduct leading to disruption of electronic networks or information systems. ▪ Negligent or intentional conduct leading to the damage of DHB electronic information, computing/networking equipment, and resources.
Excessive private usage	▪ Excessive use of DHB computer resources for private purposes. (Excessive use as determined by the appropriate line manager or department head).
Staff Information about Public use of the DHB Network	▪ Due to potential security risk, patients and members of the public are not permitted to access the Internet / worldwide web via the DHB network. This includes wired and wireless mediums. WiFi hotspots not associated with the DHB may be used provided the user is using the device in an approved zone. The device must be turned off if instructed to do so by a member of staff.

Electronic Mail and E-Communications

Access to Electronic Mail (e-mail)

Access to DHB e-mail is a privilege that may be wholly or partially restricted without prior notice and without consent of the user:

- If required by an applicable law or policy.
- If a reasonable suspicion exists that there has been, or may be, a violation of law or policy.
- If required to protect the integrity or operation of the e-mail system or computing resources, or when the resources are required for more critical tasks, as determined by an appropriate management authority.

Access to the e-mail system requires approval by an appropriate management authority (e.g. department head, system administrator, etc).

E-mailing of Clinical Information

Emailing of clinical, staff and DHB-related financial information may only be e-mailed to confirmed e-mail addresses, and only where there is no other secure method of record transfer. All precautions **must** be taken to ensure that the e-mail is going to the correct recipient. These precautions include:

- Ask recipient to send a test e-mail to confirm his or her address so you can reply with the required information.
- Send a test e-mail to the recipient and phone to confirm delivery (before sending information).

Note: Users uncertain of an e-mail address should contact the Service Desk, extn 9888 or (03) 470 9888, before sending any clinical information.

Inspection & Monitoring

The DHB **may** permit the inspection, monitoring, or disclosure of e-mail, computer files, and network transmissions when:

- Required or permitted by law or by other Southern DHB policy.
- The DHB or its designated agent reasonably believes that a violation of law or policy has occurred.
- Necessary to monitor and preserve the functionality and integrity of the e-mail system or related computer systems or facilities.

All users agree to co-operate and comply with DHB requests for access to, and copies of, e-mail messages or data when access or disclosure is authorised by this policy

	or other applicable policies, or required or allowed by law.
Strain on Services	Activities that may strain the e-mail or network facilities more than can be reasonably expected are in violation of this policy. These activities include, but are not limited to, sending chain letters; 'spam', or the widespread dissemination of unsolicited e-mail; 'letter bombs' to send the same e-mail repeatedly to one or more recipients; and use of download clients such as 'µTorrent'.
Confidentiality	Confidentiality of e-mail and other network transmissions cannot be assured. Therefore all users should exercise caution when sending personal, financial, confidential, or sensitive information by e-mail or over the network.

Privacy and Security

Logging and Monitoring	Network storage and network activities from workstations connected to the network are routinely logged and monitored. These activities include: ▪ Use of passwords and user accounts accessed. ▪ Time and duration of network activity. ▪ Web pages accessed. ▪ Network software accessed. ▪ Data storage volume limits. ▪ E-mail volume limits.
Detailed Session Logging	In cases of suspected violations of DHB policies, including unauthorised access to computing systems, the IS department may authorise detailed session logging. This may involve a complete keystroke log of an entire session (recorded what is being typed). In addition, an appropriate management authority may authorise searching of user files to gather evidence on a suspected violation (management may approve the monitoring of a user and/or their PC without their knowledge). Random audits of systems and user accounts may also be undertaken at any time.
Responsibility for Data Security	Information Services run daily back-ups of all **network** data that can be restored if required.
Restriction of Access to Sensitive Data	All DHB departments should ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords restricting access to information should be changed on a regular basis, and systems should be developed and implemented to make sure that password records are regularly updated by

	appropriate managers.
Right to Examine Computers and Equipment	DHB-owned computers and equipment may be examined to detect illegal software and to evaluate the security of the network at any time.

Violations and Enforcement

Reporting Violations	Any actual or suspected violation of the rules listed above should be brought to senior management's attention immediately. There is no recourse to repudiation (denial), since users are required to understand this policy before the use of DHB resources.
DHB Response to a Reported Violation	Upon receiving notice of a violation, the DHB may temporarily suspend a user's privileges and/or move or delete the allegedly offending material pending further investigation. A user believed to have violated these policies and procedures will be notified of the charge and have an opportunity to respond before the DHB determines an outcome and any further action that may be taken. If the DHB believes it necessary to preserve the integrity of facilities, user services, or data, it may temporarily suspend any account, whether or not the account user is suspected of any violation. Violations at Southern DHB will be dealt with according to the: ▪ Code of Conduct and Integrity (Regional) (18679) ▪ Disciplinary Policy (Regional) (55569)

Associated Documents:

- Code of Conduct and Integrity (Regional) (18679)
- Release of Patient Information Policy (21414)
- Health Records Policy (Otago) (10798)
- Fraud Policy (25546)
- Retention Schedule - General Disposal Authority for District Health Boards (45026)