Communications - Use & Management of Misuse of NSW Health Communications Systems

Summary Provides guidance and direction about the mechanisms required to minimise inappropriate use and the controls required to monitor the use of NSW Health communications systems and devices.

Document type Policy Directive

Document number PD2009_076

Publication date 19 November 2009

Author branch eHealth & ICT Strategy Branch

Branch contact (02) 8644 2213

Review date 30 June 2018

Policy manual Not applicable

File number 07/8049-4

Previous reference N/A

Status Active

Functional group Corporate Administration - Governance, Communications, Purchasing Personnel/Workforce - Conduct and ethics

Applies to Area Health Services/Chief Executive Governed Statutory Health Corporation, Board Governed Statutory Health Corporations, Affiliated Health Organisations, Affiliated Health Organisations - Declared, Public Health System Support Division, Community Health Centres, Dental Schools and Clinics, NSW Ambulance Service, Ministry of Health, Public Health Units, Public Hospitals

Distributed to Public Health System, Divisions of General Practice, Health Associations Unions, NSW Ambulance Service, Ministry of Health, Private Hospitals and Day Procedure Centres

Audience All staff

Secretary, NSW Health

USE AND MANAGEMENT OF MISUSE OF NSW HEALTH COMMUNICATION SYSTEMS

PURPOSE

- To provide a consistent definition across NSW Health regarding what constitutes appropriate and inappropriate use of NSW Health communication systems and devices.
- To provide guidance and direction about the mechanisms required to minimise inappropriate use as well as the controls required to monitor the use of NSW Health communication systems and devices.
- To provide a framework for identifying and responding to alleged misuse, to be applied in conjunction with the requirements of current NSW Health policies for managing allegations involving misconduct.

MANDATORY REQUIREMENTS

Each NSW Health agency must have:

- Effective systems and procedures in place to prevent the misuse of NSW Health communication systems and devices.
- Adequate controls to monitor and audit the use of NSW Health Communication systems and devices and to detect prohibited use.
- Documented procedures in place to effectively respond and investigate alleged breaches of this Policy Directive.

IMPLEMENTATION

Roles and Responsibilities

Chief Executives

- Must ensure that the principles and requirements of this policy are applied, achieved and sustained.
- Must ensure that all staff are made aware of their obligations regarding this policy through staff orientation or other appropriate educational means.
- Must ensure that documented procedures and adequate controls are in place to monitor use of NSW Health communication systems and devices, to detect any failure to comply with this policy including clearly defined reporting procedures and identified positions with responsibilities for managing the process.
- Must ensure that there are documented procedures in place to effectively respond to and investigate alleged breaches of this Policy Directive.

Managers and Staff

- Must ensure that all their staff are made aware of, and understand this Policy Directive.
- Must ensure monitoring and, where necessary, compliance with this Policy Directive.

- Must provide leadership by example.
- Must respond to alleged or identified misuse of communication systems in accordance with this Policy and current NSW Health policies for managing allegations involving misconduct.

All Staff

- Must ensure that they keep all information they may obtain or have access to, in the course of their work, private and confidential.
- Must be efficient, economical and ethical in their use and management of communication devices and ensure their proper and secure use.
- Must not engage in any use that may be considered inappropriate, offensive, prohibited, or could potentially damage NSW Health's reputation.
- Must not seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature as it is prohibited and may result in disciplinary action.
- Must not use NSW Health communication devices for any illegal purpose including accessing, possessing, producing or transmitting child pornography. Allegations of illegal use will be notified to the Police.
- Must report breaches of this policy to an appropriate senior officer or, if appropriate, to a nominated Protected Disclosure officer (refer to current NSW Health Policy for making protected disclosures).

NSW Department of Health

The Corporate Governance and Risk Management Branch, External Relations and Employment Screening Unit (ERESU) is the area within the Department of Health that has responsibility for this Policy Directive. ERESU's responsibilities for this Policy Directive include:

- Monitoring compliance with this Policy Directive
- Keeping the Director-General informed of alleged criminal use of the NSW Health Communication systems, where it involves child pornography.

Any comments about this Policy Directive or the associated tools and templates should be addressed to ERESU telephone (02) 9391 9654 or email cgrm@doh.health.nsw.gov.au.

REVISION HISTORY

Version	Approved by	Amendment notes
November 2005 (PD2005_632)	Director-General	New policy setting out permissible and prohibited use of NSW Health communication systems.
November 2009 (PD2009_076)	Deputy Director-General Health System Support	Replaces PD2005_632.

ATTACHMENTS

1. Use and Management of Misuse of NSW Health Communications Systems Procedures

Use and Management of Misuse of NSW Health Communication Systems

NSW HEALTH
PROCEDURES

Issue date: November 2009

PD2009_076

CONTENTS

1 BACKGROUND

1.1 Introduction

Patients, clients and staff of the NSW public health system have a right to expect that staff working within the Health System will be lawful, ethical and efficient in their use and management of NSW Health communication systems and devices.

To ensure this occurs, NSW Health agencies must have appropriate mechanisms and controls in place to prevent, identify and manage inappropriate use of NSW Health communication systems and devices.

This policy has been developed to assist Chief Executives, human resource managers and line managers in the implementation of consistent controls and mechanisms across NSW Health to promote the efficient and appropriate use of NSW Health communication systems and devices.

This policy confers certain privileges and responsibilities in relation to employee use of NSW Health communication systems and devices (such as telephones, mobile phones, computers, videoconferencing systems, personal digital assistants (PDAs), facsimiles, the Internet, Intranet and email) that are provided for business purposes.

Adherence to this policy should support the achievement of the organisational goal of providing safe, high quality health services, and minimise corporate governance risks that arise through non-compliance.

Failure by NSW Health staff to comply with this Policy Directive may result in access to NSW Health communication systems being withdrawn and disciplinary action being taken.

1.2 Principles

This Policy recognises the following principles, which are also reflected in the NSW Health Code of Conduct:

- communication systems and devices in NSW Health are provided for work use
- all work related information must be kept private and confidential
- every member of staff has a responsibility to be lawful, ethical and efficient in their use of public property and services
- every member of staff has a responsibility to be productive in the use of their work time
- staff are also private citizens with individual personal needs and obligations, who may need to make occasional use of employer communication systems for personal purposes
- there is a reasonable limit to the extent to which employer communication systems may properly be used for personal purposes which is determined by management and is reflective of the principles inherent in balancing work and family responsibilities
- staff should be provided with policies that clearly outline their rights and obligations on the use of communication systems and devices
- inappropriate or unlawful use by staff of communication systems and devices can, if made public, damage the reputation of and public confidence in NSW Health, and
- the use of NSW Health communication systems will be monitored and breaches of this Policy Directive will be investigated and may result in disciplinary action.

2 PERMISSIBLE USE OF NSW HEALTH COMMUNICATION SYSTEMS AND DEVICES

NSW Health's communication systems and devices are only to be used for work use and permissible personal use.

2.1 Work use

NSW Health's communication systems and devices are provided to staff for purposes related to the work and business of NSW Health. They are available for staff to communicate with each other, and with persons external to NSW Health, where there is a legitimate reason to communicate relevant to the work and business of NSW Health.

2.2 Permissible personal use

Personal use of NSW Health communication systems and devices is permissible where:

- the personal use is on a reasonable, responsible and limited basis and does not interfere with the effective and efficient performance of work responsibilities, or
- the use occurs during legitimate work breaks, such as lunch breaks or outside work hours, or except in other limited circumstances such as making contact with, or being contactable for family purposes, or
- there is no inappropriate or unlawful use, or
- the use does not impact on the availability of services for work or business use by others, or
- the use occurs outside an individual's work hours, with the permission of the appropriate manager, for the purposes of pursuing courses for which learning and development leave has been granted by the employer, or
- the use is by accredited union delegates for union activities.

Staff and managers should exercise judgment and fairness on reasonable personal use, and have regard as appropriate to the NSW Government's policies on balancing work and family responsibilities.

Managers are responsible for:

- identifying within their workplace what constitutes permissible personal use in accordance with the principles contained in this policy
- communicating these expectations to their staff
- reviewing, monitoring and managing the level and type of personal use.

Industrial Relations instruments such as awards can contain conditions relating to the availability of communication devices, particularly telephones. They can provide for accredited union delegates to be given reasonable access to facilities such as communication devices. *Nothing in this policy overrides the rights contained in industrial instruments.*

In addition, under the *Workplace Surveillance Act 2005,* policies dealing with email and Internet access cannot prevent the delivery of an email or access to a website merely because:

- the email was sent by or on behalf of a union or an officer of a union; or
- the website or email contains information relating to industrial matters (within the meaning of the *Industrial Relations Act 1996).*

Personal use of employer communication devices is not considered private: Staff using NSW Health's communication systems do not have the same personal privacy rights as they would have using their own private communication systems.

All users of NSW Health communication systems and devices need to be aware that their use of these systems, and particularly the use of email and Internet, will be monitored, consistent with the relevant provisions of the *Workplace Surveillance Act 2005* and, where appropriate, investigated as part of NSW Health's responsibility to implement appropriate control mechanisms. Staff suspected of abusing personal use of employer communication devices are liable to have their use reviewed, and may be asked to explain and account for such use.

Where possible to do so, NSW Health agencies must arrange for all outgoing emails to include a disclaimer making it clear the opinions expressed are those of the sender and do not represent either NSW Health or the NSW Government's view. A standard disclaimer reads:

'*Unless explicitly attributed, the opinions expressed in this email are those of the author only and do not represent the official view of [NSW Health agency] nor the New South Wales Government.'*

NSW Health organisations will not be held liable for any losses incurred as a result of permissible personal use of NSW Health communications devices.

2.3 Economic use

NSW Health staff are required to use the most economical and efficient means of communicating when using NSW Health communication systems. Staff should keep short any communication which is time charged; this applies equally to calls made from standard telephones as well as calls made from mobile telephones. Economic use is also required for all other devices.

To reduce unnecessary power consumption of computer equipment, staff must completely shut down their workstations before leaving work.

2.4 The use of personal communication systems and devices

This policy is focussed on the use of NSW Health communication systems and devices. Staff members generally should not use personal communication systems or devices for work related business, however it is acknowledged that at times, this may be necessary.

The principles enshrined in this Policy, the Code of Conduct and other relevant policies including those covering privacy and the protection of children, patients and clients apply to work related business conducted on personal communication devices.

Staff members are not allowed to use personal communication devices (or other equipment that records images) in the workplace to take images, photos or videos of NSW Health clients or patients unless they have explicit approval from their manager and the consent of the client or patient.

Where reimbursement of costs is being sought for the use of personal communication devices, authorisation must be obtained from the appropriate manager.

3 PROHIBITED USE OF NSW HEALTH COMMUNICATION SYSTEMS AND DEVICES

The use of NSW Health communication systems and devices is prohibited where the following circumstances are involved:

- inappropriate use
- use involving pornographic, sexually explicit or offensive material, or
- unlawful use, which involves breaches of Commonwealth or State laws.

It is recognised that links to some Internet sites may result in unexpected access to inappropriate material and that unsolicited email messages may be received with inappropriate content. Any staff member who inadvertently accesses or receives significantly inappropriate material is required to report the details to the local Information Services Director so that any necessary improvements to strengthen Internet and email filtering can be made, and delete the material.

Staff members who receive such emails must not distribute them further.

3.1 Inappropriate use

The inappropriate use of communication systems involves activities ranging from excessive personal use through to possession or transmission of offensive or inappropriate images or information.

3.1.1 Excessive personal use

Excessive personal use involves spending long periods of time using the communication systems for purposes unrelated to work or using the communication systems to access, transmit or download large volumes of material that is unrelated to work.

Excessive personal use is measured by its impact on the effective and efficient performance of work duties, the impact on the availability or provision of services and/or any cost factors associated with the personal use.

Excessive inappropriate personal use of the Internet includes intentionally downloading or emailing to others unauthorised software, lengthy files containing images, live pictures or graphics, such as computer games, music files, the accessing of radio or television stations broadcasting via the Internet. Such use increases the load on the network and can degrade the service to other staff with a genuine work need to use the Internet.

3.1.2 Offensive or otherwise inappropriate use

NSW Health communication systems and devices must not be used by staff to create, transmit, store or access any material that:

- could damage NSW Health's reputation or good standing in the community
- is misleading or deceptive, could potentially result in victimisation, harassment or bullying, is able to lead to criminal or civil liability, or could be reasonably found to be, offensive, threatening, intimidating, abusive, or defamatory.
- is liable to discriminate against, harass or vilify colleagues, patients/clients or the public, on the grounds of sex, pregnancy, marital status, age, race (including colour), nationality, descent or ethnic background, religious background, disability, illness, HIV/AIDS, homosexuality or transgender.

Staff may be individually liable if they assist others who use NSW Health communication systems and devices to discriminate against, harass or vilify colleagues or any member of the public.

Bullying or harassment involving the use of NSW Health communication systems and devices by NSW Health staff will be treated in accordance with existing NSW Health grievance, harassment or bullying management policies and procedures and may result in disciplinary action.

Staff must not use NSW Health communication systems and devices:

- to intentionally generate, send or receive e-mail chain letters
- to transmit offensive jokes or send junk programs etc
- for the transmission of any non-work related material to or on behalf of political parties
- to participate in any form of gambling
- for any personal commercial or business purposes unrelated to their employment or engagement with NSW Health, or
- to engage in any form of computer hacking, including illegally accessing other computers
- to access chat rooms, unless approved by a responsible manager on the basis that access is appropriate for NSW Health work purposes
- to connect any personal or non-work laptops, disk drives, PDAs, or stand-alone or wireless modems, to any NSW Health communication system or device, unless they have obtained prior written permission from the local Information Services Director. Permission should be provided on a case-by-case basis consistent with NSW Health IT security and standards.

It is acknowledged that there are circumstances where staff use USB devices for work related purposes. However there are certain risks associated with the use of these devices. These include risks to the confidentiality of patient information and risks that files uploaded from the devices may contain viruses and other malware. Use of these devices must be in accordance with the policies and procedures of the local health organisation's Information Security Management System and must meet the requirements of the health organisation's virus protection arrangements. Approval to use such devices shall be on a case-by-case basis and subject to approval at the appropriate level within the health organisation. Where USBs are used, all files stored on them that contain confidential information must be password protected.

Where a genuine work related reason exists that requires access to sites or material, or the transmission of material, that would normally be regarded as inappropriate (such as to investigate misconduct, or to manage complaints or litigation) approval from the relevant manager must be obtained and documented. If genuine work reasons require an employee to access material that would normally be regarded as inappropriate, such access should be undertaken in a suitably private environment and a record of that access documented.

If inappropriate use of any NSW Health communication system or device is established, disciplinary action may be taken against the staff member, ranging from removal of access to any NSW Health communication systems and devices through to termination of employment or engagement in more serious cases. Refer to the Management of Misuse Matrix Web Tool for the appropriate range of penalties.

NSW Health reserves the right to audit and remove any inappropriate material from its computer resources without notice.

Any alleged inappropriate use of NSW Health communication systems and devices should be handled in accordance with current NSW Health policies on managing allegations involving misconduct.

3.2 Pornographic, sexually explicit or offensive material

All staff are explicitly prohibited from using NSW Health communication systems and devices to seek out, access, store, display or transmit pornographic or sexually explicit material, or material that depicts, expresses or deals with matters of nudity, cruelty or violence in a way that a reasonable person would generally regard as offensive.

The display or transmission of offensive or pornographic material may be considered unwelcome conduct of a sexual nature which constitutes sexual harassment.

Staff should be aware that such use may constitute a criminal offence (see section 3.4).

Where there is alleged inappropriate use of NSW Health communication systems and devices involving pornographic, sexually explicit or offensive material, Chief Executives may suspend a member of staff from duty, or take other administrative action, while the matter is being investigated. In determining whether to suspend a staff member, each case must be decided on its merits following a risk assessment and in accordance with current NSW Health policies on managing allegations involving misconduct.

Staff should be aware that where inappropriate use of NSW Health communication systems and devices involving pornographic, sexually explicit material or offensive material is established, disciplinary proceedings may result in termination of their employment or engagement**.** Refer to the Management of Misuse Matrix Web Tool for the appropriate range of penalties.

3.3 Reporting alleged use involving pornography, sexually explicit or offensive material

In cases of alleged inappropriate use involving pornographic, sexually explicit or offensive material, the NSW Health agency may need to notify:

- The Independent Commission Against Corruption (ICAC) where there are reasonable grounds for believing the matter concerns corrupt conduct
- The Department of Health, if required in accordance with the NSW Health Policy on Incident Management

Alleged inappropriate use involving pornographic, sexually explicit or offensive material should be managed in accordance with current NSW Health policies on managing allegations involving misconduct and any other relevant policies, such as the current NSW Health policy on Reporting Possible Corrupt Conduct to the Independent Commission Against Corruption or any other existing grievance, harassment or bullying management policies.

3.4 Unlawful use of NSW Health communication systems and devices

3.4.1 Child pornography

Under Section 91H of the *Crimes Act 1900,* it is an offence liable to imprisonment, for a person to produce, disseminate, obtain or possess child pornography. Under Sections 474.19 and 474.23 of the Commonwealth *Criminal Code Act 1995,* it is an offence to use a carriage service to access, transmit, make available or distribute child pornography material. A carriage service means a service for carrying communications by means of guided or unguided electromagnetic energy and includes computers, mobile phones (cameras) and fax machines.

Under the *Crimes Act*, child pornography is defined as:

> material that depicts or describes, in a manner that would in all the circumstances cause offence to reasonable persons, a person under (or apparently under) the age of 16 years:
>
> (a) engaged in sexual activity, or
>
> (b) in a sexual context, or
>
> (c) as the victim of torture, cruelty or physical abuse (whether or not in a sexual context).

It is acknowledged that staff members may receive unsolicited "pop-up" child pornographic or other offensive material while accessing legitimate Internet sites. If this occurs, the staff member must note down the URL address, delete the material and report it immediately to their supervisor to report to the IT Services Manager.

The IT services Manager will determine what action needs to be taken, and where appropriate, will lodge a complaint with the Australian Communications and Media Authority (ACMA) online@acma.gov.au who are responsible for the regulation of broadcasting, radio communications, telecommunications and online content.

3.4.2 Reporting alleged unlawful use involving child pornography

Where it is identified or suspected that there has been some unlawful use of NSW Health communication systems and devices involving child pornography, **the NSW Police must be contacted immediately**. If possible, the staff member's PC/hard drive should be quarantined without warning so that there is no opportunity for files to be deleted, the computer to be switched off or on or other evidence tampered with. Contact may also need to be made with the health agency's IT Services with the view to blocking the staff member's access to email and the Internet.

Seek Police advice before initiating an internal investigation or alerting the staff member.

Special care must also be taken to ensure that any alleged child pornography images are not unnecessarily transmitted or disseminated within the NSW health agency, that they are contained and that only a limited number of nominated senior staff members are involved in any investigation and that the process for making any decisions or assessment of the material is clearly documented as part of the investigation.

Any administrative action, taken against a staff member while the matter is being investigated, must be in accordance with current NSW Health policies on managing allegations involving misconduct.

In addition to notifying the NSW Police, the NSW health agency must notify:

- the Department of Health (Corporate Governance and Risk Management Branch)
- the NSW Ombudsman (refer to current NSW Health policy on managing child related allegations, charges and convictions).

If the NSW Police decide not to proceed with an investigation or do not pursue criminal charges, the NSW health agency must still complete an internal investigation.

Any suspected use of NSW Health communication systems involving possible child pornography must be handled in accordance with current NSW Health policies on managing allegations involving misconduct, the disciplinary process and current NSW Health policy on managing child related allegations, charges and convictions against employees. Refer to the Management of Misuse Matrix Web Tool for the appropriate range of penalties.

3.4.3 Other unlawful use (not child pornography)

The use of any NSW Health communication systems and devices to access, make, receive or send fraudulent, abusive, threatening, defamatory or other unlawful images or material is prohibited. Staff must not intentionally access, create, transmit, distribute, or store any offensive or unlawful information, data or material that violates Commonwealth or State laws.

Unlawful use also includes the recording of conversations without proper authorisation under relevant legislation, such as the *Surveillance Devices Act 2007.*

All staff have a responsibility to ensure that their use of NSW Health communication systems and devices does not constitute unlawful use.

Staff who receive any threatening, intimidating or harassing telephone calls or electronic messages or images should immediately report the incident to their supervisor or manager.

3.4.4 Reporting unlawful use (not child pornography)

Where unlawful use is suspected, the NSW health agency must notify:

- The NSW Police
- The Independent Commission Against Corruption (ICAC) if there are reasonable grounds for believing the matter concerns corrupt conduct
- The Department of Health, if required in accordance with current NSW Health policies on Incident Management

If the NSW Police decide not to proceed with an investigation or do not pursue criminal charges, the NSW Health Agency must still complete an internal investigation.

Any suspected unlawful use of NSW Health communication systems or devices should be handled in accordance with current NSW policies on managing allegations involving misconduct and any other relevant policies, such as current NSW Health policies on the disciplinary process, reporting corrupt conduct to the Independent Commission against Corruption, or any other existing grievance, harassment or bullying management policies.

4 RESPONDING TO ALLEGED MISUSE OF NSW HEALTH COMMUNICATION SYSTEMS

4.1 General information

Misuse of NSW Health communication systems and devices can represent a loss of employee productivity and a need for management time to be involved in investigations and possible discipline processes. It may also involve breaches of confidentiality, damage to business image and exposure to legal liability.

All alleged breaches of this Policy Directive need to be addressed and resolved within the context of the relevant legislation, industrial instruments, principles of procedural fairness, and in accordance with current NSW Health policies on managing allegations involving misconduct.

Any response to an alleged breach should be proportionate to the seriousness of the alleged breach and the potential penalties that could be imposed if the breach is sustained. The Management of Misuse Matrix Web Tool provides advice on determining the seriousness of the alleged breach.

NSW health agencies must have in place documented procedures for dealing with alleged breaches of this Policy Directive. Such procedures should include:

- clear reporting responsibilities for staff
- identified positions with responsibilities for dealing with alleged breaches
- specific procedures for dealing with alleged unlawful use (i.e. child pornography)

4.2 Allegations concerning the Chief Executive or senior staff members

Where an allegation concerns a Chief Executive, the Department's Corporate Governance and Risk Management Branch must be notified immediately. This Branch will assist in determining the appropriate course of action, including assessing the ongoing risk to patients, clients and other staff, assessing whether any external agencies may need to be notified, and whether an external investigator should undertake an investigation.

Where an allegation concerns senior staff members, the Chief Executive may need to handle any investigation, risk management decisions or external notifications.

4.3 Allegations concerning a staff member employed in another NSW Health agency

Where the allegation concerns a staff member from another NSW Health agency, information should be forwarded for action to the Chief Executive of the employing NSW Health agency. The Department of Health may also need to be notified in accordance with the requirements of NSW Health policies on Incident Management or any other relevant NSW Health policy.

4.4 Collecting evidence in computers

A computer is designed to store a number of documents in different ways. It is important to get expert help to search a computer for documents. Specialist technical/forensic experts can make exact copies of computer hard drives to enable the analysis of information on the computer without the original computer.

4.5 The Management of Misuse Matrix Web Tool

The Management of Misuse Matrix Web Tool is a guide to assist in determining the seriousness of the alleged breach and the range of penalties that may be imposed. The tool is intended to promote consistent and fair outcomes for staff members across NSW Health that has been found to have breached this Policy Directive.

The tool reflects the different roles that the staff member may play in an alleged breach. The range of penalties available reflects whether the staff member has played an active participant role in the alleged breach or whether they have been the recipient of uninvited data which they have deleted. The tool acknowledges that staff members may receive uninvited material but that they have a responsibility to take appropriate steps to minimise the risk of further uninvited inappropriate material.

The factors to consider when determining the appropriate penalty include:

- the nature of the material involved
- the frequency of the conduct involved
- the role and type of use by employee

- the extent to which the person involved has clinical duties which involve patient contact
- the extent to which the person involved has supervisory responsibilities which require setting an example to other staff
- any relevant previous disciplinary action
- any mitigating circumstances

The current NSW Health policies for managing allegations involving misconduct, including the Policy Directive for the Service Check Register must be consulted regarding decisions around taking administrative action during an investigation or disciplinary action at its conclusion.

5 MONITORING OF NSW HEALTH COMMUNICATION SYSTEMS AND DEVICES

5.1 General information

NSW Health agencies may monitor, copy, access or disclose any information or files that are stored, processed or have been transmitted using NSW Health equipment and services. Staff should be aware that any information stored, processed or transmitted using NSW Health communication systems is the property of NSW Health and not the individual.

Chief Executives have a responsibility to ensure that appropriate controls and security are in place before authorising on-line Internet access. All requests and decisions relating to the authorising of such access must be documented and retained to facilitate scrutiny or audit.

Access to the Internet must only be through officially approved mechanisms, through a NSW Health agency firewall.

As a matter of principle, utilisation by NSW Health staff of Yahoo, Hotmail, Webmail and other similar media is not supported. The policy of NSW Health is to phase-out use of these media. These are a common entry point for SPAM, viruses, and Trojans and offensive material. Staff should use the standard email interface and application provided and secured by NSW Health.

Where arrangements have been approved for working at home or from a remote location, Chief Executives should ensure that any such arrangements comply, where possible, with the requirements of this Policy Directive and that of policies covering Flexible Work Locations. Work related emails should not be forwarded to personal email accounts as a means of circumventing protocols established for remote access to NSW Health networks.

5.2 Monitoring of the use of NSW Health Communication Systems and Devices

NSW Health agencies are to have procedures in place to ensure that Internet usage and email activity by staff is adequately monitored in order to:

- prevent de-standardisation of the computer network because of the downloading or use of unauthorised software or other devices
- ensure compliance with NSW Health policies, including this Policy Directive
- prevent inappropriate or excessive personal use of NSW Health property
- investigate conduct that may adversely affect NSW Health or its staff or be unlawful.

These procedures must take into account:

- the *Workplace Surveillance Act 2005*

- the need to observe privacy rules relating to personal information (refer to the Information Protection Principles set out in the *Privacy and Personal Information Protection Act 1998* and the Health Privacy principles set out in the *Health Records Information and Privacy Act 2003*);
- the current NSW Health Policy on Privacy
- the need to be able to link Internet sites accessed with the user identification, and generate reports with this information, and
- the establishment of appropriate processes to review these reports.

5.3 Workplace Surveillance Act 2005

Under the *Workplace Surveillance Act 200*5, NSW Health is required to inform staff in writing that computer surveillance will be occurring on an ongoing and continuous basis by means of software or other equipment that monitors or records computer usage, including, but not limited to, the sending and receipt of emails and the accessing of Internet websites.

To meet this requirement, a login screen must be used for all computers in NSW Health, which explicitly states that such monitoring will occur, and that access to Internet websites and delivery of emails may be prevented where there is material involved that is inappropriate or unlawful.

In the case of the preventing of delivery of an email sent to or from a NSW Health work email address, staff are to be given notice (*an automated prevented delivery notice)* as soon as practicable that delivery of the email was prevented, and told how they might request delivery of the email if it is work related.

A prevented delivery notice should not be provided where:

(a) the email was a commercial electronic message within the meaning of the *SPAM Act 2003* of the Commonwealth, or

(b) the content of the email or any attachment to the email would or might have resulted in an unauthorised interference with, damage to or operation of a computer or computer network operated by the employer or of any program run by or data stored on such a computer or computer network, or

(c) it has been identified that the email or any attachment to the email would be regarded by reasonable persons as being, in all the circumstances, menacing, harassing or offensive.

Orientation programs for new staff must include advice that ongoing computer monitoring and surveillance will occur.

5.4 Login Screen

To ensure that all staff accessing network services are conversant with the conditions governing their use, all NSW Health agencies must display a login screen each time staff login to their computer. The authorised content of the login screen is at **Appendix 1**.

5.5 Authentication of Network Access

The use of NSW Health computers should be capable of being monitored. Staff should only access the Internet and email services by means of a unique, individual username and confidential password that must not be shared with other users.

It is acknowledged that generic accounts[1] may be required in some circumstances. These accounts should only have access to a pre-approved list of internet sites to be determined by the

[1] Generic accounts are accounts that may be used by several users without the details of individual users being provided.

Chief Information Officer of the Health organisation in question with approval given at the appropriate level. Full access to the Internet or to applications that require authentication for these accounts should only be permitted if the user of the account is identified. Access to domain services from generic accounts is permitted.

Only currently employed staff are to have access to email and Internet services. When a person leaves the employ of the health service there must be procedures in place to remove all computer access to email and intranet, including remote access. Agencies are to have in place a system for the annual review of email access to identify any ex-employees who still have access.

5.6 Recording staff use of NSW Health Communication Systems

Records of all Internet sites accessed are to be kept in server log files. These log files are to record, at a minimum, the username of the person, the IP address of the workstation, the URL of the site accessed, the volume of data downloaded from the site and the date/time of the access. Similarly, log files of inbound and outbound Internet email message details are also to be kept, recording sender, recipient, subject, and message size, attachments and date/time group.

In many cases on-line storage space restrictions will limit the time log files can be stored on the server. However, log files must be kept either in on-line storage or on backup media for at least one year from the time of logging, and be available for inspection when required. Each agency is to have processes in place to examine or audit log files for improper use.

Under the *State Records Act 1998*, work communications sent electronically become official records, subject to statutory record keeping requirements.

Electronic records are subject to the same standards of record keeping that apply to paper records, and can be subpoenaed or 'discovered' during legal processes. Some electronic records that cannot be maintained in hard copy form without loss of content or meaning may be best maintained in electronic form, although it may be more appropriate for electronic records that require preservation to be printed out and filed in hard copy.

Sending an email from a network account is a business transaction and is similar to sending a letter on an agency's letterhead. Email transactions should be handled with the normal courtesy and discretion of other modes of communication.

All NSW Health agencies must have policies in place to ensure that staff are aware that electronic work communications are official records and should be appropriate, professionally written, saved and managed accordingly (refer to Guidelines for the Use of Emails by NSW Health staff Web Tool).

For further assistance, refer to the NSW State Records Authority's policy documents on 'Electronic Record Keeping' and 'Electronic Messages as Records'.

5.7 Automatic content filtering and virus checking

5.7.1 Emails

Emails, both inbound and outbound should be scanned for viruses, inappropriate content and certain types of file attachments.

It is acknowledged that there are many legitimate business purposes for NSW Health staff to receive and send email messages with movie, video and/or sound files attached. It is also acknowledged that many email messages with movie, video and/or sound files attached may not be work related and that health organisations may wish to block them. Blocking of movie/sound/ video files is encouraged where feasible and where not in conflict with business needs. Management of blocking is the responsibility of each health organisation. Emails should be scanned by 'content' and 'title' using designated key words developed within each Health organisation to block inappropriate material.

There should be a facility to quarantine blocked emails into a designated post box where an authorised person can monitor and sample content on a regular basis. An automated message should be generated to inform the staff member that the email has been blocked, and details of the actions they may take to unblock the information if it is work related.

Where a staff member receives unsolicited inappropriate emails, the staff member must delete the email and where they know the source of the email they must inform the sender that they have deleted the email and that they are not to send any further such emails. The staff member should retain evidence where possible of notifications to senders not to send such emails.

5.7.2 Internet

Access by staff members to sites that contain unacceptable information is contrary to the Code of Conduct and can place the reputation of NSW Health at risk. Other sites can lead to staff members spending large amounts of time on unproductive non-work-related purposes.

Access to such sites should be blocked by installing appropriate software. Several products that enable blocking of such sites are available from NSW Government contracts. Products should be selected that record attempts to access non-approved sites and can issue alerts to Network Administrators. There should be a facility to alert a staff member that they have tried to access a blocked site with advice on the procedure to apply to have access where there is a legitimate work related reason to do so. The number, addresses and types of inappropriate sites change constantly and it is not possible to present a durable, exhaustive list. Health organisations are responsible for the installation of appropriate software to ensure that access to inappropriate Internet sites are blocked. Health organisations should ensure that the sites blocked are reviewed and updated regularly to ensure currency.

Approval to access a blocked site should be provided by an authorised person upon written endorsement of the requesting staff person's senior manager. There should be a facility to allow a Systems Administrator to selectively enable or disable access on a site-by-site basis according to the endorsed approval process in place.

5.8 Security of NSW Health Communication Systems

5.8.1 Network security

Messages conveyed through NSW Health communication systems and devices can be intercepted, traced or recorded by persons outside NSW Health. Mobile telephone calls can be intercepted. Users cannot have an expectation of privacy. Access through an Internet gateway can be readily traced and any Internet site visited can keep a record of a visit.

To safeguard the integrity of usernames and passwords, each employee should keep his or her password confidential. Except in exceptional circumstances, such as to effect urgent after hours access to a document, no one should access the network, Internet or email services using the username and password of another person, or permit or otherwise enable a username and password to be used by someone else.

If there is a suspicion that a password has been compromised, or a password has been provided to another staff member for urgent access to a document, the password must be changed as soon as possible.

In order to minimise security risks to communication systems, NSW Health agencies must have in place appropriate controls, such as:

- rules for staff around creating effective passwords and for regular changing of passwords
- systems to test the security of staff passwords
- firewalls and filters

- classification and transmission protocols for business records
- regular risk assessments
- monitoring the use of communication systems
- compliance with the appropriate sections of the Australian and New Zealand Standard 27002 as it applies to the secure transmission of personal health information, and
- providing personal computers with time-based locking mechanisms, which are password activated.

NSW Health agencies should ensure that mobile communication devices which are easily stolen, such as pagers, mobile telephones, personal digital assistants (PDAs) and laptop computers, have in-built and activated security features such as password or personal identification number protection and these security features must be used by all staff.

NSW Health agencies must ensure that all work related laptop computers have the agency's standard operating environment installed.

Information regarding access to NSW Health's computer and communication systems, such as passwords, usernames, dial-up phone numbers and email address lists, should be considered to be confidential information and should not be divulged without authorisation.

The NSW Health Policy on Electronic Information Security Policy addresses NSW Health's obligation to protect sensitive information including the provision of appropriate levels of security across all the electronic information systems and networks for which it is responsible.

5.8.2 Workstation security

Employees should never leave their workstation unattended while it is logged on at the NSW Health network, corporate applications or email system. When leaving a desk unattended, employees must lock their workstation or activate a password-protected screen saver. When leaving a workstation for an extended period of time it is recommended that employees save any open files and close any corporate applications or systems before starting the screen saver. Alternatively, employees should log out of their workstation.

The NSW Policy on protecting people and property provides further information.

5.9 Mobile telephones

Mobile telephones can be used to connect to the Internet, they can be used as facsimiles or as electronic messaging systems as well as to take and record images. They provide benefits that can significantly add value to service delivery.

Staff should understand that this policy directive applies equally to the use of work mobile phones as to any other type of communication device.

Chief Executives have a responsibility to pay particular attention to properly authorising and monitoring the use of mobile telephones (including use of personal mobile phones for work related matters) and should ensure there are procedures in place regarding:

- **The provision of mobile phones to staff**. Mobile telephones are only provided to staff in circumstances where there is a demonstrated work need, such as a requirement to be contactable after hours or where there is a requirement to work outside the usual office environment.
- **The use of mobile telephones while driving**. Using hand held mobile phones while driving is an offence. NSW Health agencies will not be responsible for any fines incurred by staff improperly using mobile telephones. Being involved in an accident while using a hand held mobile telephone could negate any insurance claim. Chief Executives should

authorise the installation of hands-free mobile telephones in employer-owned vehicles where an operational need can be clearly demonstrated. Alternatively, mobile telephones should be linked to voice mail, a message bank, or an answering service.

- **Security issues regarding the use of mobile phones**. Staff should know that mobile phone calls can be intercepted, and that extra precautions must be taken to secure mobile phones as they are easily stolen, such as activating in-built security features.
- **The use of mobile phones in public places**. Staff should be aware of confidentiality and privacy issues when using mobile phones to conduct business in public places.
- **The use of mobile phones for taking images/pictures/videos**. The taking of images/photos/videos using NSW Health devices must be in accordance with the requirements of this policy, the code of conduct and other policies around the privacy and protection of children, patients and clients. In addition, while "permissible personal use" applies to photos stored on mobile phones, non-work-related images or videos are not to be transmitted from NSW Health mobile phones.

6 GLOSSARY

Blocking and filtering The terms 'blocking' and 'filtering' are often used as synonyms for the technologies that prevent access to particular types or specific pieces of the content that are available on the Internet. 'Blocking' refers to the techniques used within routers that stop Internet traffic based on its addresses, and 'filtering' to those techniques that stop access to content based on its content. The term filtering may also be used as a general term for both blocking and filtering.

Chat rooms are discussion groups that people can enter and leave at any point in time. Some chat rooms have restricted membership, but others are public. It is commonplace for chat room visitors to adopt a pseudonym.

Chief Executive means the Chief Executive of a NSW Health agency.

Communication system includes, but is not restricted to the following systems and devices:

- cellular telephones
- computers connected to any network or data circuit
- electronic date interchange, EDO email
- facsimile transmissions
- filming devices
- Internet
- Intranet
- paging devices
- personal digit assistants (PDAs)
- videoconferencing systems
- satellite communications equipment
- telephones - landlines and mobiles
- wireless devices.

Electronic mail (also known as email) is a computer-based message sent over a communications network to one or more recipients. It may be transmitted with attachments such as electronic files containing text, graphics, images, digitised voice, digitised video or computer programs.

Firewall is a security barrier generally erected between an organisation's computer network and the Internet to protect internal organisational data. It is a system that can be implemented in both hardware and software, or a combination of both, to prevent unauthorised access to or from a private network. Firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet, especially intranets.

Corporate Governance and Risk Management Branch (CGRM) is a Branch of the NSW Department of Health that provides Health Services with a range of governance and risk management responsibilities. This responsibility includes advice and support in responding to child-related and criminal allegations, charges and convictions, and monitoring performance in responding to such matters. The Branch also coordinates employment screening for the NSW Health system. Enquiries to the branch should be made to telephone External Relations and Employment Screening Unit on (02) 9391 9654 or email to cgrm@doh.health.nsw.gov.au.

Internet is a worldwide loose affiliation of interconnected computer systems (involving government, commercial, academic and private providers) through which an individual with a personal computer can access services and information. Services available through the Internet include, but are not necessarily confined to, electronic mail, Telnet and the World Wide Web (www). The NSW Government encourages public sector agencies to use the Internet as a means for improving service delivery.

Intranet is an internal (restricted) network that uses Internet technology.

Malware short for *malicious software*, is software designed to infiltrate or damage a computer system without the owner's informed consent. The term means a variety of forms of hostile, intrusive, or annoying software or program codes. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

Mobile telephones are mobile phones that are long-range, portable electronic devices used for mobile communication. In addition to the standard voice function of a telephone, current mobile phones can support many additional services such as SMS for text messaging, email, packet switching for access to the Internet, and MMS for sending and receiving photos and video.

Newsgroups There are thousands of newsgroups worldwide, covering almost every conceivable topic. Users need to become subscribers to newsgroups to be able to access the news, and any subscriber can post material to a news group. Newsgroups started off as public e-mail discussion forums but are also used as data repositories.

NSW Health is a reference to the NSW public health system that includes:

- the NSW Department of Health and the Health Administration Corporation
- Health Professional Registration Boards
- Institute of Psychiatry
- the NSW Ambulance Service, and
- Area Health Services, Statutory Health Corporations, the Public Health System Support Division (Health Support Services, Health Infrastructure and IMET), Affiliated Health Organisations in respect of their recognised services and establishments, Public Hospitals, Community Health Centres, Dental Schools and Clinics, and Public Health Units.

NSW Health agency or organisation is a reference to any of the entities contained under the definition of NSW Health.

Pager refers to a small telecommunications device that receives short radio messages (either numeric or alphanumeric). When a pager captures a message it is usually accompanied by a beep to alert the person carrying the pager. The device is also sometimes called a "beeper'. Pagers that can both receive and send messages have been recently developed.

PDAs Personal digital assistants (PDAs) are handheld computers that were originally designed as personal organisers, but have become much more versatile over the years. PDAs are also known as pocket computers or palmtop computers. Many PDAs can access the Internet, intranets or extranets via Wi-Fi, or Wireless Wide-Area Networks (WWANs). One of the most significant PDA characteristic is the presence of a touch screen.

Procedural fairness In terms of investigations and risk assessments, procedural fairness involves informing the employee of the substance of the allegation against them, providing the employee with an opportunity to put forward their case, making reasonable inquiries during the investigation, considering all relevant evidence, ensuring that there is no conflict of interest; acting fairly and without bias, conducting investigations and risk assessments without undue delay, and maintaining good records in relation to these matters.

SPAM Is the abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired. While the most widely recognised form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, mobile phone messaging spam, internet forum spam and junk fax transmissions. Spam is also called junk mail. Some email clients or servers have spam filters, which try to delete or move the spam messages.

Staff member means any individual having employee functions or acting in a similar capacity, including any volunteer, consultant, visiting medical practitioner, contractor or employee of a contractor who is provided with access to communication devices owned by a NSW Health. The term covers Chief Executives.

USB (**Universal Serial Bus**) is a tool to establish communication between devices and a host controller, usually personal computers (PC). USBs can connect computer devices such as mice, keyboards, digital cameras, printers, personal media players, flash drives, and external hard drives.

World Wide Web (WWW) The World Wide Web is a user friendly interface enabling the user to access millions of sources of information located on the Internet through a Web browser such as Internet Explorer and through Web search engines such as Google. Web documentations are written in "hypertext", a system that allows for text and graphical "links" to documents and files spread across the Internet.

7 WEB TOOLS

The following tools are available from the NSW Department of Health Intranet site at: http://internal.health.nsw.gov.au/cgrm/cger/communication_systems_tools.html

1. Mandatory login screen for all NSW Health computer systems
2. Relevant Legislation and Policies
3. Guidelines for the use of email by NSW Health staff
4. Management of Misuse Matrix

Appendix 1: Self Assessment Compliance Checklist

Checklist for the implementation of the Use and Management of Misuse of NSW Communication Systems Policy Directive

Requirement:	*Self Assessment:*		
	In development	***Partial implementation***	***Mature***
A. STRATEGIC FUNDAMENTALS			
1. The NSW Health agency has developed a plan to implement the requirements of this policy.	❑	❑	❑
2. There are resources and support to implement the requirements of the policy and an appropraite officer has been identified as responsible for the regular monitoring of progress.	❑	❑	❑
3. Key Performance Indicators (KPIs) are developed to monitor and measure the implementation	❑	❑	❑
B. INTEGRATION INTO NORMAL BUSINESS SYSTEMS			
4. The requirements of this Policy Directive are included in all orientation programs for new staff.	❑	❑	❑
5. Current staff are given information about the requirements of this Policy, including the requiirement to report alleged breaches of this Policy.	❑	❑	❑
6. All computer access has the mandatory Log IN screen and requires authentification of acess	❑	❑	❑
7. There is automatic content filtering and virus checking for electronic communication and access to the Internet.	❑	❑	❑
8. There are procedures in place regarding the use of mobile phones as required in the Policy.	❑	❑	❑
9. There are documented procedures for managing alleged breaches of this Policy.	❑	❑	❑

Requirement:	Self Assessment:		
	In development	*Partial implementation*	*Mature*
10. *Access to generic network accounts do not include access to the internet*	❑	❑	❑
11. *There is a process for removing access to NSW communicatoin sytems when staff members cease to be employed*	❑	❑	❑
12. *There is a system in place to alert staff members that they have tried to access a blocked internet site and details of the procedure in place for them to apply for access.*	❑	❑	❑
13. *There is a procedure in place for staff to apply to have access to blocked internet sites where access is required for work purposes*	❑	❑	❑
14. *All computers are set to activate a password proetected screen saver when inactive for any time.*	❑	❑	❑
C. ORGANISATIONAL IMPLEMENTATION			
15. *Managers are aware of their repsonsibilities for ensuring that their staff understand the requirements of this Policy.*	❑	❑	❑
16. *There are systems in place for monitoring and auditing the use of NSW Health communication systems.*	❑	❑	❑
17. *There are rules in place for staff around creating effective passwords and systems to test the security of passwords.*	❑	❑	❑
18. *There are systems for keeping records of all Internet sites accessed by staff.*	❑	❑	❑