Justice Health and
Forensic Mental Health Network

Justice Health NSW Policy

Acceptable Use of Communication Systems

Issue Date: 06 June 2024

Together for
Healthier Tomorrows

Acceptable Use of Communication Systems

Policy Number 2.002

Policy Function Leadership and Management

Issue Date 06 June 2024

Next Review Date 06 June 2028

Risk Rating Medium

Summary This policy ensures effective guidelines and procedures are in place to prevent the misuse of communication systems and devices and investigate alleged breaches in accordance with NSW Health Policy Directive PD2009_076 *Communications - Use & Management of Misuse of NSW Health Communications Systems*.

Responsible Officer Chief Digital Health & Information Officer

Applies to
☒ Administration Centres
☒ Community Sites and programs
☒ Health Centres - Adult Correctional Centres or Police Cells
☒ Health Centres - Youth Justice Centres
☒ Long Bay Hospital
☒ Forensic Hospital

CM Reference POLJH/2002

Change summary
- Hyperlinks/reference updates and only minor changes to wording/grammar

Authorised by Chair, Policy Steering Committee

Revision History

#	Issue Date	Number and Name	Change Summary
5	Jun 24	2.002 Acceptable Use of Communication Systems	• Hyperlinks/reference updates and only minor changes to wording/grammar
4	Apr 21	2.002 Acceptable Use of Communication Systems	• Social media changes • References to Ministry policy • Email changes
3	Apr 16	2.002 Acceptable Use of Communication Systems	• Tablets and Wifi referenced • Social media authorization changed to ED

2	Mar 12	2.002 Acceptable Use of Communications Systems	• Amalgamated hardware, software, email, internet and offsite ICT policies • Reformatted as an Implementation Guide to PD2009_076 Updated title
1	Dec 08	2.002 Acceptable Use of ICT Resources	• Updated due to the opening of the new Prison hospital, Forensic hospital and the Administration building • Updated title

PRINT WARNING

Printed copies of this document, or parts thereof, must not be relied on as a current reference document.

Always refer to the electronic copy for the latest version.

Justice Health and Forensic Mental Health Network

PO BOX 150 Matraville NSW 2036

Tel (02) 9700 3000

http://www.justicehealth.nsw.gov.au

Table of Contents

1. Preface 5
2. Policy Content 5
2.1 Roles and Responsibilities 5
2.2 Mandatory Requirements 6
3. Procedure Content 7
3.1 Acceptable Use of Communication Systems 7
3.1.1 Permissible Personal Use 7
3.1.2 Acceptable Use of Email Proxy Access 7
3.1.3 Acceptable Use of the Intranet and Internet 8
3.1.4 Acceptable Offsite Usage 8
3.2 Prohibited Use of Communications Systems and Devices 9
3.2.1 Prohibited Use of ICT Equipment/Resources 10
3.2.2 Prohibited Use of Email 10
3.2.3 Prohbited Use of the Internet and Intranet 12
3.3 Monitoring 12
3.3.1 Notification 13
3.3.2 Virus Checking and Content Filtering – Email 14
3.3.3 Monitoring of Internet Usage Virus Checking and Content Filtering 14
3.3.4 Citrix Access 15
3.4 Security 15
3.4.1 User Accounts and Passwords 15
3.4.2 Physical/Data Security 16
3.5 Information Requests under GIPA Act 16
4. Definitions 16
5. Related Documents 17

1. Preface

The NSW Ministry of Health (The Ministry) has established policy on the appropriate use and management of misuse of communication systems across all health agencies. Justice Health NSW (JHNSW) is committed to ensuring the appropriate use of Information Communications Technology (ICT) resources provided for its activities in accordance with NSW Health Policy Directive PD2009_076 *Communications - Use & Management of Misuse of NSW Health Communications Systems* (hereafter PD2009_076).

JHNSW ICT resources include, but are not limited to:

- Desktops, laptops/notebooks, tablets
- Printers, Scanners and Multi-function devices
- Email and all other software
- Internet and Intranet access
- Modems and routers
- Removable media such as memory sticks, USB devices, digital cameras, mobile phones, media players, CDs, DVDs, and similar portable storage devices.

This policy outlines the acceptable use and prohibited use of all JHNSW ICT resources by any employee, contractor or other relevant parties, regardless of where those duties are performed and regardless of whether they are work related or non-work related.

2. Policy Content

2.1 Roles and Responsibilities

All staff are responsible for:

- Being aware of and abiding by requirements in this policy and PD2009_076.
- Reporting inappropriate communication or alleged breaches of this policy to their line manager or the Chief Digital Health & Information Officer.
- Advising the ICT Service Desk of any emails received that appear to be unsolicited commercial electronic messages under the *Spam Act 2003* (Cth) (herein known as the *Spam Act 2003*).

Managers are responsible for:

- Investigating all alleged breaches of this policy.
- Submitting a *Change Of Access & Termination* (COAT) form when direct reports relocate within the organisation or terminate employment. This will ensure ICT access is adjusted or terminated and relevant data archived.
- Assuming full responsibility for all electronic data associated with departing staff members and instructing departing staff to capture official records in HPRM or other official records management system where applicable.

The Chief Information Officer is responsible for:

- Preparing regular reports to the Executive on general internet use in the organisation
- Responding to alleged breaches to this policy.

2.2 Mandatory Requirements

JHNSW ICT systems and devices are provided to staff for work purposes and to effectively and efficiently communicate to internal and external persons. As a condition of using ICT resources, staff must:

- Read and abide by requirements outlined in this policy and PD2009_076
- Not download, email, store, print or display anything that could reasonably be construed, in the opinion of JHNSW, as menacing, harassing, offensive or inappropriate to a reasonable person unless the correspondence is necessary to promote clinical care, for example patient complaints
- Not give the impression they are representing, giving opinions or otherwise making statements on behalf of JHNSW or part thereof, or any officer of JHNSW, unless they are explicitly authorised to do so
- Not copy, reproduce or distribute (including by email) copyright material without written permission of the copyright owner, except as provided for by the principles of fair dealing. This includes compliance with the spirit and intent of software licensing requirements
- Indemnify the JHNSW against any and all claims or liabilities, directly or indirectly, relating to their use of ICT resource

JHNSW supports the directive from the Commissioner of Corrective Services NSW that removable storage media such as USB memory sticks, CDs and DVDs, SIMs and other related media are expressly prohibited at correctional centres, unless otherwise approved by endorsed authorities. Staff in sites other than correctional and Youth Justice centres may be provided with removable media subject to the approval by the requestor's line manager and in line with JHNSW purchasing standards.

Alleged breaches of this policy must be addressed and resolved within the context of relevant legislation, industrial instruments, principles of procedural fairness and in accordance with policies on managing allegations of 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. Managers should refer to the *Management of Misuse Matrix Web Tool* for advice on determining the seriousness of the alleged breach. Any user engaging in any activity that is deemed by local management to be in breach of this policy may have their access to communication systems revoked. Alleged breaches that would violate Australian or State laws or regulations must be forwarded by the Chief Information Officer to the Director Workforce, or where appropriate, the Chief Executive. Where unlawful use of communications systems and devices is identified or suspected, the NSW Police Force will be immediately notified and relevant systems and equipment quarantined.

Any documents or other sources of information compiled, recorded or stored in written form, on film, by electronic process, or in any other manner or by any other means will constitute a record under the *State Records Act 1998*, and must be captured, managed and disposed of in accordance with this Act. JHNSW records are also subject to laws concerning disclosure

and privacy, including the *Government Information (Public Access) Act 2009*, the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*.

3. Procedure Content

3.1 Acceptable Use of Communication Systems

JHNSW ICT systems and devices must only be used for work purposes and permissible personal use as defined in this policy and PD2009_076. Regardless of whether JHNSW or non JHNSW ICT resources are used, users accept responsibility for using ICT resources in a way that is ethical and acknowledge responsibility for all documents, information and content they access and cause to be transmitted or stored, held, copied, downloaded, displayed, viewed, read or printed through software or on hardware as a consequence of this service.

Staff must note considerations outlined below when using JHNSW communication systems and comply with other instructions as released by ICT staff.

3.1.1 Permissible Personal Use

Personal use of JHNSW email or the Internet is permissible where it is clear the user is not representing JHNSW or its affiliates and satisfies the following:

1. Personal use is on a reasonable, responsible and limited basis that is consistent with the effective and efficient performance of work responsibilities
2. Use occurs during legitimate work breaks, such as meal breaks or outside work hours, except in other limited circumstances such as making contact or being contactable for family purposes
3. There is no inappropriate or unlawful use
4. The use does not impact the availability of services for work or business use by others.

Personal use does not extend to intentionally downloading or emailing to others unauthorised software, files containing images, live pictures or graphics, such as computer games, music files; nor radio or television streamed via the Internet.

3.1.2 Acceptable Use of Email Proxy Access

All JHNSW email account holders are able to provide other JHNSW email account holders proxy access to their accounts. This may include access to the user's inbox, calendar etc. Proxy access may be granted access at varying levels, e.g. read access only, write access, etc.

Proxy access to JHNSW email accounts should be limited only to people of trust, and to the level required. JHNSW email account holders are responsible for managing and checking who they have provided proxy access to and the associated levels of access provided. ICT cannot be held responsible for security breaches resulting from access to, or use by, the account owner's proxy user.

Distribution Groups / All User Emails

JHNSW email account holders may request ICT to create email distribution groups, with a minimum of five (5) internal staff members in the group. Distributions groups require a

group owner who is responsible for maintaining the group. An email distribution group enables the user to send an email to one account (e.g. Senior Managers) and all staff in that group will receive the email.

'All staff' emails (emails sent to all persons with a JHNSW email account) or 'all site' emails may be useful to convey important messages, however excessive or unwarranted use of all staff emails, particularly messages with large or multiple attachments, can cause network congestion and in extreme circumstances may significantly hamper the operation of the email and other JHNSW systems. Staff who wish to distribute an 'all staff' email must seek approval from the CE, relevant Executive Director or the Chief Information Officer.

3.1.3 Acceptable Use of the Intranet and Internet

The Internet and Intranet may be used for work use and permissible personal use. This is regardless of whether the Internet or Intranet is accessed on a JHNSW site, via corporate or third party WiFi, or external connection to the JHNSW or any Internet Service Provider (ISP), and regardless of equipment used.

Internet

By accessing the Internet through JHNSW systems, users acknowledge that:

1. They will report breaches of system security when they become aware of them
2. They will immediately report any unauthorised use of their account
3. Some documents, information and content on the Internet may contain controversial or offensive material over which the JHNSW has no control and cannot be held responsible.
4. JHNSW accepts no responsibility for any non JHNSW documents, information or content, from any source whatsoever, that user access on the Internet, and JHNSW gives no warranty as to the suitability, accuracy, currency nor fitness for any particular purpose of that material.

Intranet

JHNSW Intranet is an internal operational tool for use by JHNSW and NSW Health employees and third party service providers approved by the Chief Information Officer. Nothing therein may be displayed, reproduced, stored or transmitted in any form or by any means, electronic or otherwise for any purpose or use other than those for which it was intended, or for use outside the JHNSW, without the written permission of the CE.

3.1.4 Acceptable Offsite Usage

JHNSW ICT resources may be used offsite for work-related duties in approved circumstances. This may include remotely connecting to the JHNSW's corporate network and resources via an approved access method. Such ICT resources include home computers, laptops, tablets, printers, and software.

When undertaking work-related duties offsite, security must be a paramount consideration. Staff with remote access to the organisation's network and resources have an obligation to manage this securely at all times to protect the corporate network and data stored within. This includes ensuring user credentials are not compromised, and

accessed systems are exited and active windows completely closed at the completion of work.

JHNSW ICT Resources

ICT will provide support for JHNSW ICT resources used offsite for work-related duties if they are used in an appropriate manner as outlined in this and related ICT policies.

JHNSW ICT resources must not be used for personal use offsite under any circumstances.

Non JHNSW ICT Resources

With approval, non JHNSW ICT resources may be used for work purposes when an employee is unable to access a JHNSW ICT resource. Naturally, personal use of non JHNSW ICT resources is permitted in designated breaks or outside business hours, and this policy does not cover that use.

ICT will not provide support for non JHNSW ICT equipment and resources used offsite for work- related purposes.

Staff accessing network resources from non JHNSW ICT equipment must report lost or stolen devices to ICT for risk assessment purposes.

Specific prohibitions and considerations for this policy include where non JHNSW ICT resources of current and former JHNSW employees, contractors and other relevant parties are disposed of, such persons are required to ensure that no JHNSW data is retained on that equipment.

3.2 Prohibited Use of Communications Systems and Devices

Regardless of whether JHNSW or non JHNSW ICT resources are used onsite or offsite, activities that constitute prohibited use include, but are not limited to:

- Creating, transmitting, storing, accessing, or soliciting material that could reasonably be construed, in the opinion of the JHNSW, to be abusive, obscene, threatening, profane, sexually oriented, racially offensive, defamatory, contain context that is illegal in nature, discriminatory in nature, inciting criminal offences, encouraging the use of controlled or illicit substances, containing offensive images, likely to cause distress to some individuals/cultures or harassing or disparaging others based on their race, national origin, gender, transgender, sexual orientation, age, religious beliefs or political beliefs, or any other use deemed to be inappropriate or prohibited by JHNSW, where such material is not a legitimate part of work
- Deliberate, unauthorised corruption or destruction of ICT systems or data (including deliberate introduction or propagation of computer viruses)
- Deliberate, unauthorised access to facilities or data
- Unauthorised use of data or information obtained from information systems
- Transmission or use of material that infringes copyright held by another person or JHNSW. Users found to have violated copyright may be subject to disciplinary proceedings as well as civil proceedings involving damages, and to criminal penalties as provided for by Commonwealth and State laws
- Violation of software licensing agreements
- Transmission of unsolicited commercial or advertising material

- Deliberate impersonation of another individual on the network by the use of their login access or other means
- Violation of the privacy of personal information relating to individuals, such as staff and patients
- Unauthorised disclosure of confidential information
- Harassing or threatening other individuals
- Operation of an ICT system or other equipment, which presents a threat to the confidentiality, integrity or availability of JHNSW ICT services
- Unauthorised attempts to identify or exploit system weaknesses
- Unauthorised attempts to make JHNSW ICT systems or services unavailable
- Use of JHNSW facilities to gain unauthorised access to third party computing facilities
- Use of JHNSW facilities in unauthorised attempts to make third party computing facilities unavailable
- Use that significantly degrades system performance for other users
- Installing non-approved software such as games and screen savers
- Storage of personal files such as music, videos and photos. ICT reserves the right to remove such files without notice.

3.2.1 Prohibited Use of ICT Equipment/Resources

Under no circumstances can JHNSW ICT equipment and resources be connected to or installed on non JHNSW ICT equipment/resources, or used to transfer JHNSW data to non JHNSW ICT equipment/resources. Conversely, under no circumstances can non JHNSW ICT equipment and resources be connected to or installed on JHNSW ICT equipment/resources, or used to store JHNSW data (including memory sticks, mass storage devices, CDs, DVDs and personally owned computers). ICT will not support JHNSW ICT equipment and resources that are used offsite where any of the above happens. Any repair or replacement costs for damage to JHNSW ICT equipment and resources resulting from the above circumstances must be paid for by the user.

3.2.2 Prohibited Use of Email

The stipulations for prohibited use of email outlined in this policy and PD2009_076 are applicable to JHNSW and non JHNSW email accounts used by staff at work or offsite for work-related duties. These include:

- Spamming or Spam - The sending of non-work related and unsolicited messages to an individual or group of email users
- Letter Bombing - The repeated sending or forwarding of email messages to a user or group of users
- Where sensitive, classified or in-confidence communications are to be sent electronically security should be paramount and NSW Health Secure File Transfer should be utilised.

JHNSW is not responsible for:

- The content or nature of messages received by users of the email system
- Protecting users from receiving electronic mail they may find offensive
- Offering any warranty to users as to the confidentiality and security of the system
- The offering of any warranty as to the validity of authorship or authenticity of the purported sender of any email received by users.

Auto Forwarding

Auto-forwarding email is not an acceptable or standard working practice. Where possible an Out of Office message should be setup in the account in preference to the use of auto-forwarding.

For security reasons auto forwarding JHNSW email accounts to non NSW Health email accounts is prohibited in all circumstances.

Spam

All email messages that users send from a JHNSW email account must comply with the *Spam Act 2003*. Users must be aware of the requirements of this Act.

Under the *Spam Act 2003*, users must include accurate contact details in every message sent. This may include an automatic signature.

The *Spam Act 2003* distinguishes between commercial and factual electronic messages, and is determined by the purpose for which it was sent. For example, the following would be commercial electronic messages:

- Unsolicited commercial electronic messages offering to supply, advertise or promote goods/services (for example, promotions, special offers, and product updates) or business opportunities.
- Factual electronic messages that provide a link to a commercial website, including email newsletters, updates, and bulletins.
- The *Spam Act 2003* applies to the sending of all electronic messages, but is particularly relevant to the sending of commercial electronic messages to email address lists. Under the *Spam Act 2003* users may send a commercial electronic message only if:
- The consent of the recipient can be construed, a functional unsubscribe facility allows the recipient to withdraw their consent at any time, and any requests to unsubscribe are actioned within 5 days.
- The message relates to JHNSW goods and services, and is sent to current or former staff, contractors or related parties, or their households.

Under the *Spam Act 2003* users must not supply, acquire or use “address-harvesting software” or address lists generated from this software. “Address-harvesting software” is software that searches the Internet for email addresses.

Users must take appropriate action to ensure emails comply with the *Spam Act 2003*. The sending of any emails outside these guidelines is not authorised by JHNSW and users may be liable for any breach of the Act if they send such emails. The *Spam Act 2003* sets financial and other penalties depending on the severity of the breach.

3.2.3 Prohbited Use of the Internet and Intranet

In addition to the prohibitions noted in this policy and PD2009_076, it is expressly prohibited to use Internet and Intranet services provided by the JHNSW for private commercial gain. Under no circumstances are JHNSW Internet and Intranet services to be used:

- To facilitate or circulate any form of advertising or sponsorship
- For the sale of private goods or services
- For private monetary gain.

JHNSW reserves the right to prohibit access to Internet material that, in the judgment of the JHNSW may be considered:

- Likely to be offensive
- Likely to cause affront or alarm
- Obscene
- Defamatory
- Likely to advocate, incite or procure a criminal action.

3.3 Monitoring

JHNSW's Chief Executive or the Chief Digital & Health Information Officer at the request of an Executive Director or Director Workforce may inspect, monitor and disclose data from traffic-monitoring systems when:

- Required to by, and consistent with, the law
- There is reasonable cause to believe that violations of the law, JHNSW policy or inappropriate use of the service have occurred.
- There is a suspicion of misuse or policy breach.

Please refer to the related sub-section in NSW Health Policy Directive PD2009_072 *State Health Forms*, for further details on monitoring requirements 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 policy directives.
- Prevent inappropriate or excessive personal use of Government property.
- Investigate conduct that may adversely affect any Health agency or their staff or be unlawful. NSW Health notes that monitoring processes must take into account:
- The provisions of the *Workplace Surveillance Act 2005* dealing with computer surveillance
- 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 Health Privacy Principles set out in the *Health Records and Information and Privacy Act 2002*.
- *NSW Health Privacy Manual for Health Information*

- NSW Health Policy Directive PD2026_001 *Digital Health Cyber Security*.
- The need to link Internet sites accessed with user identification, and generate reports with this information.
- The establishment of appropriate processes to review these reports.

3.3.1 Notification

In accordance with PD2009_076, the JHNSW must notify staff that it will monitor staff use of ICT resources, such as Internet and email.

Such notification must occur in a way that meets the obligations of the *Workplace Surveillance Act 2005*. This notification must indicate that it is the policy of all NSW Health entities (including JHNSW) that computer surveillance will occur on an ongoing 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).

Such notification will be in writing, which is defined in the *Workplace Surveillance Act 2005* to include notice by email. A login screen will be used for all computers in NSW Health (including JHNSW devices) that explicitly states that such monitoring will occur. New staff should also be informed at orientation programs that computer surveillance will occur.

The notification provided to staff must also indicate that access to external websites and delivery of emails may be prevented where there is material involved that is inappropriate or unlawful.

In the case of preventing delivery of an email sent to a work email address, staff must be given a prevented notice as soon as practicable that delivery of the email has been prevented, unless delivery of the email was prevented in the belief that, or by the operation of a program intended to prevent the delivery of an email on the basis that:

a) The email was a commercial electronic message within the meaning of the Spam Act of the Commonwealth

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

c) The email or any attachment to the email would be regarded by reasonable persons as being, in all the circumstances, menacing, harassing or offensive.

Login Screen

When logging on to the network each person is presented with the screen titled “Justice Health and Forensic Mental Health Network – Acceptable Use of ICT Resources.” The person must accept or reject these terms. Failure to accept assumes you will not comply and therefore will not be permitted to continue accessing services in that session.

Where JHNSW staff, contractors and related parties have been notified that monitoring may occur, the login screen should explicitly state that such monitoring will occur. To this end, by accepting the login screen the user may assume they have been notified that monitoring may occur.

Logging usage

JHNSW retains and may monitor usage logs of various ICT resources, which may reveal information such as which Internet sites have been accessed by employees, contractors and related parties, and the email addresses of those with whom they have communicated. JHNSW will not engage in real-time surveillance of ICT resource use, or monitor the content of messages sent or received by its employees, contractors and related parties unless there is a suspicion of misuse. Information contained in logs will not be provided to external third parties except under compulsion of law.

3.3.2 Virus Checking and Content Filtering – Email

One of the main routes by which viruses propagate themselves is through executable programs hidden or embedded in email attachments. A recipient may trigger a virus by opening an attachment, which causes the malicious application to run. The action required to execute the package is so simple that a recipient might open the attachment and trigger the virus without even realising it. JHNSW blocks attachments that are or may include executable programs to limit the threat of viruses being spread via email. By refusing executable attachments via email the threat of a virus outbreak in the organisation's ICT infrastructure is reduced.

For security purposes, ICT prohibits certain file types from being attached to emails. If an email with a banned attachment type comes into JHNSW from an external source it is quarantined at entry into NSW Health and will not be released. No warning is passed back to the sender.

All incoming and outgoing emails are scanned for viruses and inappropriate content, and may be blocked and logged if appropriate. There is two-layer scanning available, as follows:

- Email is scanned at JHNSW email gateway
- The desktop scanning agent automatically scans any file that is being executed. For example, if the user double-clicks the attachment in an email or opens it from a location it has been saved to.

If users are concerned that an attachment may be malicious they may save the file to a location, then go to that location and right click on the file and select scan for viruses.

3.3.3 Monitoring of Internet Usage Virus Checking and Content Filtering

Any downloads, including files, from a website are assessed at the gateway for viruses, and files will be blocked if infected with a virus.

All files downloaded from a site are scanned for viruses and inappropriate content, and may be blocked and logged if appropriate. There is two-layer scanning available, as follows:

- Scanning at the network gateway.
- The desktop scanning agent automatically scans any file that is being executed, i.e. if the user saves the file to a location and opens it from there, or if it is executed/run directly from the website.

If users are concerned about a downloaded file they may save the file to a location, then go to that location and right click on the file and select scan for viruses. Users should also

note that JHNSW prohibits and blocks the downloading of files that may cause damage and are malicious. These may include executable (EXE) and related files.

Blocking and Blocked Sites

Web content filtering software is used to allow or prohibit access to websites. Users attempting to enter a blocked site will receive a message in the browser informing them they cannot access the site.

JHNSW reserves the right to block any sites deemed unsuitable for viewing and use at work, or when connected remotely to the organisation's network. As users move around approved sites, (i.e. navigating through to sub-pages or other websites) the software continues to assess the content for its suitability, and parts of a site may be blocked.

Staff who require access to sites or content that has been blocked by filtering are to gain approval from their line manager for access, prior to contacting ICT.

Logs will be kept of internet sites accessed by staff as well as site content.

Offsite Access

Staff must abide by acceptable use requirements in this policy when working offsite and accessing JHNSW resources (such as Outlook or Internet Explorer) through an internet connection (third party cabled/WiFi or 4\5G wireless modems).

3.3.4 Citrix Access

When users are working offsite and accessing JHNSW resources (such as Outlook or Internet Explorer) through a Citrix connection, they should be aware that their use of resources may be monitored, and any websites accessed and emails sent or received will be checked for viruses and content.

3.4 Security

3.4.1 User Accounts and Passwords

- All persons with access to JHNSW ICT systems will have their own separate accounts, with a unique network user ID.
- Users are responsible for all activity initiated from their accounts, unless it is established that the activity was done by another person who gained access to the user's account through no fault of the user.
- Users are to ensure work devices are locked before when leaving their work area unattended by using alt-ctrl-del or logging off.
- Users must select passwords that cannot be easily guessed – see the *Password Guidelines* provided by ICT.
- Users must not divulge passwords to others, including other employees, contractors and related parties.
- Users must not write their passwords and store them in a visible place.
- Users are not permitted to authorise others to login using their account.
- If the security of a password is compromised, it must be changed immediately.

- Users must change their password at least every 90 days – they will be prompted by the system to do so.
- Users are prohibited from using another user's account to access any ICT resources including PAS, JHeHS, email etc.
- Users must not attempt to determine another user's password.

3.4.2 Physical/Data Security

JHNSW will endeavour to maintain the physical security of ICT resources through appropriate storage, backup, and protection from theft or damage.

All JHNSW employees, contractors and related parties are required to physically secure ICT resources carried with them or used offsite, such as laptops, tablets, mobile phones and digital cameras).

All persons with access to JHNSW ICT systems via a mobile device must report the loss of any device to the JHNSW's Digital Operations team immediately. ICT may initiate a remote data wipe where possible for any mobile device that connects to the organisation's network resulting in the loss of personal data such as contacts, photos, etc.

3.5 Information Requests under GIPA Act

Under the *Government Information (Public Access) Act 2009* (the GIPA Act), members of the public have a legally enforceable right to access government information, unless there is an overriding public interest against disclosure. All electronic records, including but not limited to emails, documents and databases generated on ICT systems, are subject to public disclosure where required under the *GIPA Act*.

Staff who hold records that fall under the scope of an access application must provide access to JHNSW 's Right to Information Officer. The Right to Information Officer will consult with relevant areas and conduct the public interest test for each record pursuant to the *GIPA Act*. Under the public interest test, unless there is an overriding public interest against disclosure, agencies must provide the information.

Staff should note it is an offence to conceal, destroy or alter records of government information for the purpose of preventing the disclosure of information as required by or under the *GIPA Act*.

4. Definitions

Must

Indicates a mandatory action to be complied with.

Should

Indicates a recommended action to be complied with unless there are sound reasons for taking a different course of action.

5. Related Documents

Legislations	*Anti-Discrimination Act 1977* *Children and Young Persons (Care and Protection) Act 1998* *Crimes Act 1900* *Spam Act 2003* *State Records Act 1998* *Government Information (Public Access) Act 2009* *Privacy and Personal Information Protection Act 1998* *Health Records and Information Privacy Act 2002* *Workplace Surveillance Act 2005* *Privacy and Personal Information Protection Act 1998* *Health Services Act 1997* *Independent Commission Against Corruption Act 1988*
Justice Health NSW Policies, Guidelines and Procedures	
Justice Health NSW Forms	*Change Of Access & Termination* (COAT)
NSW Health Policy Directives and Guidelines	PD2009_072 *State Health Forms* PD2009_076 *Communications - Use & Management of Misuse of NSW Health Communications Systems* PD2015_049 *NSW Health Code of Conduct* PD2025_021 *Managing Misconduct, Serious Performance and Child Related Concerns* PD2026_001 *Digital Health Cyber Security* Use and Management of Misuse of NSW Health Communication Systems - *Management of Misuse Matrix Web Tool* *NSW Health Privacy Manual for Health Information* Use and Management of Misuse of NSW Health Communication Systems – *Guidelines for the use of email by NSW Health staff* *Information Security Services – Service Delivery Hub* *Digital Records Preservation Policy*

Other documents and resources