Queensland Health

Use of ICT services & devices

Queensland Health Digital Standard

QH-IMP-484-1: 2021

1. Statement

This standard supports the Use of ICT services and devices Policy and the Information Security Policy by establishing the conditions that staff must abide by as an authorised user of Queensland Health's ICT services and devices.

2. Scope

This standard supports the Use of ICT services and devices policy and applies to all staff within Queensland Health. Staff is defined as employees, students, interns, volunteers, contractors, consultants, Board Members and managed service providers working for Queensland Health. Queensland Health consists of:

- the Department of Health, and
- Hospital and Health Services.

3. Requirements

All staff must be appropriately authorised prior to accessing and using departmental ICT services and devices. Authorised users are to access and use departmental ICT services and devices for their intended purposes according to the *Queensland Health Use of ICT services and devices Policy*, the Queensland Government Enterprise Architecture *Use of ICT Facilities and Devices Policy (IS38)*, the *Code of Conduct for the Queensland Public Service*, Public Service Commission *Private Email Use Policy*, relevant legislation and Department of Health or HHS policy.

All authorised users must, upon login to the network, agree to the *Conditions of use* of the computer system and in so doing, acknowledge accountability for any use of departmental ICT services and devices under their control; including internet and extranet access and email messages, and awareness that such use may be subject to audit, public scrutiny and/or disclosure.

Usage of Queensland Health's ICT services and devices includes:

1. The use of all types of communication and information devices used to access Queensland Health networks, internet and email services.
2. All information transmitted or made available via Queensland Health's intranet and email services.
3. The use of privately-owned devices connecting or attempting to connect to Queensland Health's ICT services and devices from any location.

When authorising access to Queensland Health's ICT services and devices, managers and supervisors are to ensure that access is provided to authorised users for:

1. Official work-related purposes.
2. Educational and self-development purposes consistent with government policy.
3. Professional development that is approved by appropriate senior officers.

Queensland Government

4. Limited and reasonable personal use.

Note: 'Authorised and Unauthorised Use' conditions apply regardless of whether the use occurs within work hours or outside of work hours. The ability to connect to Queensland Health ICT service or device does not in itself imply that an authorised user is permitted to access and use that service.

3.1. Inappropriate use

Inappropriate use includes, but is not limited to:

3.1.1. Staff must not use Queensland Health's ICT services and devices to intentionally capture, send, store or access inappropriate material.

3.1.2. Staff must not send or post information that is defamatory to Queensland Health, its services, staff, patients; or any other individual or organisation.

3.1.3. Staff must not use personal email accounts or messaging app to conduct government business. A Chief Executive may allow an employee or group to use private email accounts in certain situations. Refer to the Email use standard for further information.

3.1.4. Staff must not forward or email official information, including pictures or attachments, to a personal email account.

3.1.5. Staff must not deliberately perform acts that waste or monopolise computer or network resources. This includes accessing streaming or other online services (internet radio or television, sports broadcasts, simulcast, gaming, gambling) or making international calls, that are not for officially approved purposes.

3.1.6. Staff must not use Queensland Health's ICT services for unapproved commercial, lobbying, advocacy, political or fundraising activities or for personal financial gain.

3.1.7. Staff must not operate a personal or not-for-profit business(es) from work, including sale of personal property.

3.1.8. Staff must not attempt to access any system without prior authorisation. Staff must only access information systems if required for, and consistent with, the performance of their role.

3.1.9. Staff must not attempt to disable or circumvent any security measures on any system.

3.1.10. Staff must not attempt to intercept any network session or communication without proper authorisation.

3.1.11. Staff must not knowingly access, download or distribute any material that is infected with viruses or any other form of malicious software (malware).

3.1.12. Staff must not connect any unauthorised device to Queensland Health's physical network, wireless networks, VPN services or any other Queensland Health managed networks without authority to do so.

3.1.13. Staff must not connect any unauthorised removable media (e.g. USB thumb drives, portable hard drives), peripherals, or any other device to Queensland Health equipment, unless the device has been authorised for work use.

3.1.14. Written authorisation is to be obtained before taking any Queensland Health device or equipment off-site, with the exception of mobile devices that you have been authorised to use.

3.1.15. Mobile devices are to be used lawfully, safely and securely.

3.1.16. Information classified or likely to be classified as Sensitive or above must not be copied on to removable media unless encrypted with an approved encryption mechanism.

3.1.17. Staff must not use public WiFi to login to the Queensland Health network on personal or Queensland Health device.

3.1.18. Third party websites such as Dropbox, Google Drive or Apple Messages/iCloud, are not to be used to transfer Queensland Health information to other agencies.

3.1.19. Staff are not to install any unauthorised software without authority to do so. All authorised software must be licensed to Queensland Health or the relevant HHS and legitimately acquired and used in accordance with Department of Health or HHS policies, standards, and procurement procedures.

3.1.20. Staff must not procure or use any service to store or process Queensland Health information, including cloud-based IT applications, unless the service has been assessed by Cyber Security and the appropriate authorisation given.

3.1.21. Staff must not distribute copies of software licensed to Queensland Health, or a HHS or transfer Queensland Health or HHS licensed software to personal computers, without authorisation to do so.

3.1.22. Staff must not access or download or disseminate any material or records in breach of privacy, confidentiality, copyright, Intellectual Property Rights or any other legislative restrictions.

3.1.23. Staff must not attempt to masquerade or impersonate others, or otherwise use a false identity.

3.1.24. Staff are not to pass off personal views posted to the internet (including social media) as representing those of the Queensland Health and must not imply official endorsement.

3.2. Unlawful use

Unlawful use includes, but is not limited to:

3.2.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by Queensland Health or a HHS.

3.2.2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of any images including photographs from magazines, copyright music, books or other copyrighted sources for which Queensland Health, the HHS or the end user does not have an active licence is prohibited.

3.2.3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

3.2.4. Using mobile or satellite telephones when operating a vehicle in contravention to State legislation or road rules.

3.2.5. Knowingly inciting hatred towards, serious contempt for, or severe ridicule of a person or group of persons on the ground of race, religion, sexuality or gender identity of the person or members of the group.

3.2.6. Sending messages without authority that may cause people to fear for their safety or the safety of others.

3.2.7. Sending unsolicited commercial electronic messages (spamming).

3.2.8. Breaching related state and federal legislation and regulations including but not limited to:

- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- Confidentiality provisions in part 7 of the *Hospital and Health Boards Act 2011*
- Privacy principles contained in the *Information Privacy Act 2009*, including the National Privacy Principles
- *Telecommunications Interception Act 2009*.

Unlawful use may attract penalties defined under legislation including the Spam Act 2003 (Cth), Anti-Discrimination Act 1991 and Defamation Act 2005.

3.3. Criminal use

Criminal use includes, but not limited to:

3.3.1. Accessing, downloading, on-forwarding, storing or distributing child pornography.

3.3.2. Procuring or grooming persons under the age of consent for sexual purposes using government resources.

3.3.3. Breaching copyright, for example by unlicensed copying of a computer program on a computer.

3.3.4. Intercepting, accessing or altering data (hacking), or falsifying electronic documents or programs without legal authority to do so.

3.3.5. Carrying out illegal activities (e.g. such as illegal gambling, fraud, stalking and unauthorised recording) or carrying out defamatory activities.

3.3.6. Creating, or helping to create, malware (e.g. viruses, worms or Trojan horses or any other potentially harmful software) and/or loading or helping to load such software on any ICT facility or device.

3.3.7. Using any ICT facility or device to cause a 'denial of service' attack.

3.3.8. Hacking into a computer system protected by a password or other security measure to access personal or commercial information or alter that information.

3.3.9. Sending a threatening message such as a bomb threat.

3.3.10. Accessing, transmitting or making available material that promotes suicide

3.3.11. Vilifying persons on the basis of their race or religion.

Criminal use may attract penalties as defined under legislation including the *Cybercrime Act 2001 (Cth)* and the *Criminal Code Act 1899*.

3.4. Management of unauthorised use

3.4.1. On becoming aware of potential unauthorised use, managers/supervisors are to consider the nature of the potential breach and refer it to the appropriate HR Delegate to determine if further investigation is required.

3.4.2. Where unauthorised access or use has occurred, the following actions may be taken:

1. Local management action – including coaching, training and providing guidance on appropriate use.
2. Temporary or permanent modification or removal of access.
3. Disciplinary action up to and including termination of employment in accordance with Queensland Health's Discipline HR Policy E10.
4. Legal action and prosecution.

3.4.3. Use of ICT services and devices that constitutes suspected corrupt conduct is to be reported in accordance with Requirements for Reporting Corrupt Conduct HR Policy E9 or the relevant HHS equitant policy.

3.4.4. For more information on disciplinary procedures please refer to the Use of ICT training, awareness and disciplinary procedure standard.

3.5. Inadvertent or accidental access to inappropriate sites or emails

3.5.1. Staff who inadvertently or accidentally accesses unauthorised, inappropriate or offensive material using ICT services must:

1. Not store or disseminate such material by whatever means.
2. Delete such material including email messages immediately. Such action may not be considered 'unauthorised use'.
3. Advise their supervisor/manager of the event as soon as practicable.

4. Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Criminal Justice Act 1988*
- *Cyber Crime Act 2001 (Cth)*
- *Electronic Transaction Act 2001*
- *Financial Accountability Act 2009*
- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*

- *Right to Information Act 2009*
- *Telecommunications Act 1997 (Cth)*
- *Workplace Health and Safety Regulation Act 2008*

5. Supporting documents

- Use of ICT services and devices policy
  - Access control standard
  - Audit and recordkeeping standard
  - Collaboration platforms standard
  - External access standard
  - Information access, use and disclosure standard
  - Monitoring and reproting standard
  - Training, awareness and disciplinary procedure standard
  - Use of Email standard
- Anti-discrimination and vilification HR Policy E2
- Discipline HR Policy E10
- Information Security Policy
- Performance improvement HR Policy G11
- Requirements for reporting suspected corrupt conduct HR Policy E9
- Software Asset Management Policy
- Suspension of employment HR Policy E14
- Workplace conduct and ethics HR Policy E1
- Workplace Harassment HR Policy E13

6. Definitions

Term	Definition
ICT services and devices	ICT services and devices include computers (including mobile and handheld devices); telephones (including mobiles and smart phones); paging systems; BYO devices connecting to the Queensland Health network; instant messaging services; removable media; radios or other high frequency communication devices; television sets; digital or analogue recorders (including DVD and video); cameras; photocopiers; facsimile machines; printers (and other imaging equipment); electronic networks; internet; email; web mail; fee-based web services; videoconferencing equipment; collaboration platforms; ICT enabled medical devices; satellite broadcasting and ICT enabled monitoring systems
Inappropriate material	Inappropriate material includes, but is not limited to, material that is:

Term	Definition
	– pornographic – racist – discriminatory – inflammatory – defamatory – sexist – sexually explicit – obscene – abusive – threatening – offensive – harassing – likely to cause offence, or which would be considered socially unacceptable.

For further ICT definitions please refer to:

Digital policy glossary

Version Control

Version	Date	Comments
1.0	01/03/2021	New standard. Endorsed Architecture and Standards Committee. Approved by Director-General.