Queensland Health

Use of ICT services and devices

Queensland Health Digital Standard

QH-IMP-484-1

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.

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.

2. Scope

This standard applies to all staff within Queensland Health. Staff is defined as employees, students, interns, volunteers, contractors, consultants, Board and committee members, third-party providers, and managed service providers working for Queensland Health. Queensland Health consists of:

- the Department of Health, and
- Hospital and Health Services (HHS).

3. Requirements

3.1. Accessing and using ICT services and devices

3.1.1. All staff must be appropriately authorised prior to accessing and using Queensland Health ICT services and devices in line with the Queensland Health Access control standard.

3.1.2. Authorised users are to access and use Queensland Health 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.

3.1.3. 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 Queensland Health ICT services and devices under their control;

including internet and extranet access and email messages, and awareness that such use may be subject to access, audit, public scrutiny and/or disclosure.

3.1.4. Authorised users must ensure network enabled devices allocated to them are regularly connected to the Queensland Health network in order to receive security and quality updates and to maintain currency.

3.1.5. Cost centre managers must ensure all devices assigned to their cost centres that have not been issued to staff are periodically connected to the network to maintain currency.

3.1.6. Authorised users must use an approved transfer method to share information between internal and external recipients.

3.1.7. Allocated devices must be kept physically secure. Lost or stolen devices must be reported to their manager or supervisor and logged on the IT Support Portal as soon as possible.

3.2. Authorised use

3.2.1. 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. Professional development that is approved by appropriate senior officers.
3. Educational and self-development purposes consistent with government policy.
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.

3.3. Unauthorised use

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

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

3.3.3. Staff must not download and store Queensland Health information on personal devices, except as part of approved external access provisions. Refer to the External access Standard for more information.

3.3.4. Staff must not use personal email accounts or messaging apps to conduct government business. A Chief Executive may allow an employee or group to use private email accounts in certain situations. Refer to the Use of Digital Communication standard for further information.

3.3.5. Staff must not forward or email official information, including pictures or attachments, to a personal email account unless authorised by their manager or delegated custodian.

3.3.6. Staff must not craft emails or messages or construct attachments in a way that attempts to bypass content inspection software.

3.3.7. Staff must not use email messages as a method of creating legally binding contracts, unless the formal contract is attached following existing contract processes.

3.3.8. 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.

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

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

3.3.11. 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.

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

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

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

3.3.15. 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.

3.3.16. 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 approved for work use.

3.3.17. 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. Refer to the Information security classification and handling standard and the Encryption Guideline for more information.

3.3.18. Queensland Health data, except publicly available data, must not be stored on any unauthorised devices. For more information refer to Storing information on USB drives.

3.3.19. Staff must not input or upload information that is not publicly available into commercial (public) tools, such as artificial intelligence services.

3.3.20. Staff must not take any Queensland Health device or equipment off-site without prior written authorisation; except for mobile devices that you have been authorised to use.

3.3.21. Staff must not share or loan Queensland Health devices to third parties, including family members.

3.3.22. Text messaging via personal mobile phone (except for approved BYOD) should not be used to record any business decisions or information.

3.3.23. The Tik Tok application, or other applications assessed as high-risk applications, must not be installed on government owned devices and should not be used on BYOD that are accessing Queensland Health data and systems.

3.3.24. Staff must not use untrusted and unencrypted WiFi, for example public WiFi or unfiltered WiFi, to access the Queensland Health network or Queensland Health information that is not publicly available, whether it be on a personal device or Queensland Health device. This includes O365 applications to access work emails or other work-related applications.

3.3.25. Unapproved third-party services such as Dropbox, Google Drive or Apple Messages/iCloud and artificial intelligence platforms, are not to be used to transfer Queensland Health information.

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

3.3.27. Staff must not distribute copies of software licensed to the Department or HHS or transfer departmental or HHS licensed software to personal computers, without authorisation to do so.

3.3.28. Staff must not procure or use any service to store or process or use Queensland Health information, including free or trial cloud-based applications, and artificial intelligence technologies, without prior assessment of the service's risk, legislative compliance, and the delegated custodian's authorisation.

3.3.29. Staff must not access, download, or disseminate any material, information or records that would be breach privacy, confidentiality legislation, intellectual property rights (for example copyright) or any other legislative restrictions.

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

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

3.4. Unlawful use

Unlawful use includes, but is not limited to:

3.4.1. Inappropriately using Queensland Health systems or records, to access, use or disclose personal, confidential, or official information held by Queensland Health for their own personal interest, curiosity or gain.

3.4.2. Violations of the rights of any person or company protected by privacy, 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 the Department or the HHS.

3.4.3. 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 authorised and/or active[1] licence is prohibited.

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

3.4.5. Unlawfully damaging or deleting permanent, high-value or high-risk records or information that has not been captured or synced to an appropriate recordkeeping or business system.

3.4.6. Using mobile or satellite telephones, or other devices when operating a vehicle in contravention to relevant legislation or road rules.

3.4.7. 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.

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

3.4.9. Sending unsolicited commercial electronic messages (spamming).

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

- *Public Sector Ethics Act 1994*
- *Public Sector Act 2022*
- *Human Rights Act 2019*
- *Hospital and Health Boards Act 2011*
- *Information Privacy Act 2009*
- *Telecommunications Interception Act 2009*
- *Invasion of Privacy Act 1971.*

[1] Queensland Health holds government licences with copyright collecting societies in relation to internal use of copyright material (i.e., use on the intranet or emailing to other Queensland Health staff) for the purposes of the State of Queensland. For more information regarding use of copyright material owned by other parties refer to Copyright information for researchers | Queensland Health.

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

3.5. Criminal use

Criminal use includes, but not limited to:

3.5.1. Accessing, downloading, on-forwarding, storing, or distributing child exploitation material.

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

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

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

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

3.5.6. 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.

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

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

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

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

3.5.11. Vilifying persons on the basis of their race, religion, or cultural background.

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

3.6. Management of unauthorised use or access

3.6.1. On becoming aware of potential unauthorised use or access, 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.

3.6.2. 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.

3.6.3. 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 equivalent policy.

3.6.4. All suspected or confirmed unauthorised use or access involving personal information should be referred to the relevant Privacy and Confidentiality Officer at the earliest opportunity in accordance with the organisation's privacy breach management process.

3.7. Inadvertent or accidental access to inappropriate sites or emails

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

1. Not store or disseminate such material by any 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. Follow the relevant department or HHS privacy breach management process if the inadvertent use or access involves personal information.

3.7.2. Receiving unsolicited material does not constitute unauthorised use, however storage or dissemination of inappropriate or unacceptable material would constitute unauthorised use.

3.7.3. Deleting unsolicited emails not related to business activities does not constitute unauthorised disposal under the *Public Records Act 2002*.

4. Human rights

The standard aligns with the *Human Rights Act 2019*, emphasising adherence to its principles. This ensures that our operations prioritise legal compliance and respect for individual rights.

5. Legislation

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Cybercrime Act 2001*
- *Electronic Transactions (Queensland) Act 2001*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2019*
- *Hospital and Health Boards Act 2011*

- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Invasion of Privacy Act 2009*
- *Public Health Act 2005*
- *Public Interest Disclosure Act 2010*
- *Public Records Act 2002*
- *Public Sector Act 2022*
- *Public Sector Ethics Act 1994*
- *Right to Information Act 2009*
- *Telecommunications (Interception and Access) Act 1979 (Cth).*

6. Supporting documents

- Use of ICT services and devices policy
  - Audit and recordkeeping standard
  - Collaboration platforms standard
  - Information access, use and disclosure standard
  - Monitoring and reporting standard
  - Training, awareness and disciplinary procedure standard
  - Use of digital communication standard
- Data and application custodianship policy
- Data and application custodianship standard
- Discipline HR Policy E10
- Generative AI Factsheet
- Information Security Policy
  - Access control standard
  - External access standard
  - Information security classification and handling standard
- Patient Safety Alert 04/2024: Use of mobile phones by clinicians in clinical settings
- Performance improvement HR Policy G11
- Queensland Health Use of Mobile Phone Position Statement
- Requirements for reporting suspected corrupt conduct HR Policy E9
- Suspension of employment HR Policy E14
- Workplace conduct and ethics HR Policy E1.

Public Service Commission:

- Code of Conduct for the Queensland Public Service
- Disciplinary Directive (05/23)
- Private Email Use policy
- Use of Internet and email policy.

Queensland Government Enterprise Architecture (QGEA)

- Use of ICT services, facilities and devices policy (IS38)
- Information access and use policy (IS33)
- Information asset custodianship policy (IS44)
- Information Security Policy (IS18:2018)
- Records governance policy
- Use of TikTok application policy | For government | Queensland Government.

7. Definitions

Term	Definition
Artificial Intelligence (AI)	Software that is developed with one or more of: a. machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning, b. logic-based and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference, and deductive engines, (symbolic) reasoning and expert systems, or c. statistical approaches, Bayesian estimation, search, and optimisation methods and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.
Authorised use	Use by individuals who have received authorisation before operating the relevant device or service and agreed to abide by the policies, guidelines, and local practice arrangements for use of the relevant facility or device, and who have appropriately acknowledged this agreement where required.
Authorised User	Users who have received authorisation before operating the relevant device or service and agreed to abide by the policies, guidelines, and local practice arrangements for use of the relevant facility or device, and who have appropriately acknowledged this agreement where required.

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: – pornographic – racist – discriminatory – inflammatory – defamatory – sexist – sexually explicit – obscene – abusive – threatening – offensive – harassing – likely to cause offence, or which would be considered socially unacceptable.
Official information	Official information is routine information without special sensitivity or handling requirements.
Personal information	Information or an opinion (including information or opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from that information or opinion.
Privacy breach	A privacy breach occurs when there is a failure to comply with one or more of the privacy principles set out in the *Information Privacy Act 2009* (Qld) (IP Act). A privacy breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.
Third party	An individual or an organization outside of the individual agency that provides labour or services.

Term	Definition
Unauthorised use	Access that has not been authorised including use which is inappropriate, unlawful and/or criminal (refer to Use of ICT services, facilities, and devices policy (IS38) for further clarification).

For further ICT definitions please refer to:

Digital policy glossary

8. Approval and implementation

Policy Custodian	Policy Contact Details	Approval Date	Approver
Deputy Director-General eHealth Queensland	Digital-policy@health.qld.gov.au	17/10/2024	Director General

Version control

Version	Date	Comments
1.0	01/03/2021	New standard. Endorsed by Architecture and Standards Committee. Approved by the Director-General.
2.0	17/10/2024	Cyclic review undertaken See Change Table below. Endorsed IMSGC Endorsed ISC Endorsed ASC Approved Director-General.

Change Table

Section	Change
Statement	Section removed from Requirements and added to Statement: 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.
Scope	Updated to include Committee members, third-party providers

Section	Change
Requirements	New heading added: 3.1 Accessing and using ICT services and devices
	Requirements added: 3.1.4. Authorised users must ensure the network enabled devices allocated to them are regularly connected to the Queensland Health network in order to receive security and quality updates and to maintain currency. 3.1.5. Cost centre Managers must ensure all devices assigned to their cost centres that have not been issued to staff are periodically connected to the network to maintain currency. 3.1.6. Authorised users must use an approved transfer method to share information between internal and external recipients. 3.1.7. Allocated devices must be kept physically secure. Lost or stolen devices must be reported to their manager as soon as possible.
3.3 Unauthorised use	Statement removed Inappropriate use included, but is not limited to
	Requirement updated 3.3.3. Staff must not download and store Queensland Health information on personal devices, except as part of approved external access provisions. Refer to the External access Standard for more information.
	Requirement updated 3.3.5. Staff must not forward or email official information, including pictures or attachments, to a personal email account unless authorised by their manager or delegated custodian.
	New requirement 3.3.6. Staff must not craft emails or messages or construct attachments in a way that attempts to bypass content inspection software.
	New requirement 3.3.7. Staff must not use email messages as a method of creating legally binding contracts, unless the formal contract is attached following existing contract processes.
	New requirement 3.3.17. 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. Refer to the Information security classification and handling standard and the Encryption Guideline for more information.
	New requirement 3.3.18. Queensland Health data, except publicly available data, must not be stored on any unauthorised devices.
	New requirement

Section	Change
	3.3.19. Staff must not input or upload information that is not publicly available into commercial (public) tools. Such as artificial intelligence services.
	New requirement 3.3.21. Staff must not share or loan Queensland Health devices to third parties, including family members.
	New requirement 3.3.22. Text messaging via personal mobile phone (except for approved BYOD) should not be used to record any business decisions or information.
	New requirement 3.3.23. The Tik Tok application, or other applications assessed as high-risk applications, must not be installed on government owned devices and should not be used on BYOD that are accessing Queensland Health data and systems.
	New requirement 3.3.24. Staff must not use untrusted and unencrypted WiFi, for example public WiFi or unfiltered WiFi, to access the Queensland Health network or Queensland Health information that is not publicly available, whether it be on a personal device or Queensland Health device. This includes O365 applications to access work emails or other work-related applications.
	Requirement updated 3.3.26. Unapproved third party services such as Dropbox, Google Drive or Apple Messages/iCloud and artificial intelligence platforms, are not to be used to transfer Queensland Health information.
	3.3.29. Staff must not procure or use any service to store or process or use Queensland Health information, including free or trial cloud-based applications, and artificial intelligence technologies, without prior assessment of the service's risk, legislative compliance and the delegated custodian's authorisation.
3.4 Unlawful use	New requirement 3.4.1. Inappropriately using Queensland Health systems or records, to access, use or disclose personal, confidential or official information held by Queensland Health for their own personal interest, curiosity or gain.
	Requirement updated 3.4.5. Unlawfully damaging or deleting permanent, high-value or high-risk records or information that has not been captured or synced to an appropriate recordkeeping or business system.
	Requirement updated

Section	Change
	3.4.6. Using mobile or satellite telephones, or other devices when operating a vehicle in contravention to relevant legislation or road rules.
	Requirement updated 3.4.10. Added: • *Public Sector Act 2022* • *Invasion Privacy Act 1971* Removed: Confidentiality provisions in Part 7 of the.... Privacy Principles contained in the.... ....including the National Privacy Principles
3.5 Criminal use	New requirement 3.5.1. Accessing, downloading, on-forwarding, storing, or distributing child exploitation material.
	New requirement 3.5.8. Hacking into a computer system protected by a password or other security measure to access personal, confidential, or commercial information or alter that information.
	New requirement 3.5.11. Vilifying persons on the basis of their race, religion, or cultural background.
3.6 Management of unauthorised use	Heading updated 'Or access' added
	Requirement updated 3.6.1. On becoming aware of potential unauthorised use or access, 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.
3.7 Inadvertent or accidental access	Requirement updated 3.7.1. Staff who inadvertently or accidentally accesses unauthorised, inappropriate or offensive material or information using ICT services must:
	New requirement 4. Follow the relevant department or HHS privacy breach management process if the inadvertent use or access involves personal information.
	New requirement 3.7.2. Receiving unsolicited material does not constitute unauthorised use, however storage or dissemination of inappropriate or unacceptable material would constitute unauthorised use.
	New requirement

Section	Change
	3.7.3. Deleting unsolicited emails not related to business activities does not constitute unauthorised disposal under the *Public Records Act 2002.*
4. Human Rights	New requirement (Added to support the *Human Rights Act 2019*) The standard aligns with the *Human Rights Act 2019*, emphasising adherence to its principles. This ensures that our operations prioritise legal compliance and respect for individual rights.