

# Use of ICT services and devices

## Queensland Health Digital Policy

QH-POL-484

### 1. Statement

The Use of Information and Communications Technology (ICT) services and devices policy sets out the acceptable behaviour required by staff, including contract and third-party providers, when using ICT services and devices within Queensland Health.

For the purposes of this policy ICT services and devices includes, but is not limited to, computers, laptops, ICT network, ICT enabled medical devices, infrastructure, applications, portals, cloud, mobile devices, internet, storage, email, external access, collaboration services, Bring Your Own Device (BYOD), telecommunications, printers, faxes, photocopiers, and video conferencing equipment. <sup>1</sup>

### 2. Purpose

The purpose of this policy and its supporting standards is to:

- outline the general obligations and responsibilities of staff in relation to the acceptable use of ICT services and devices across Queensland Health's system, including reasonable personal use
- prevent misuse or loss of ICT services and devices and minimise risk associated with unethical behaviour
- describe the access, use, auditing, monitoring, reporting and record keeping requirements for ICT services and devices
- define the consequences of breaching this policy.

### 3. Scope

This policy 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.

---

<sup>1</sup> See Definitions for broader definition of ICT services and devices.

## 4. Principles

**Accountability and Responsibility:** Queensland Health ICT services and devices are used responsibly, including behaviour that:

- Is in accordance with the Code of Conduct for the Queensland Public Service, public sector ethics and other applicable legislation
- Does not disrupt the efficient delivery of Queensland Health's system services.

**Confidentiality and privacy:** Queensland Health ICT services and devices are protected to safeguard privacy and confidentiality, preserve data, and ensure the ongoing availability of information.

**Respect for Human Rights:** Queensland Health is committed to upholding the principles embodied in the *Human Rights Act 2019* in all aspects of its ICT operations. This includes but is not limited to the rights to privacy, freedom of expression, and access to information. All ICT initiatives and practices are designed and implemented with due consideration for the protection and promotion of human rights as outlined in the Act.

**Security:** Security policies, controls and guidelines are applied to the storage, access, processing, or data transmission, to protect information against loss, unauthorised access, use, modification, or disclosure, and against other misuse.

**Managed:** ICT services and devices are actively managed and monitored. All records created are effectively managed and preserved in compliance with relevant legislation.

## 5. Requirements

### 5.1. Use of ICT services and devices

- 5.1.1. ICT services and devices are provided to assist authorised users in the performance of their official duties, while allowing for professional and limited personal use.
- 5.1.2. In all cases, staff must abide by legislative requirements including the *Hospital and Health Boards Act 2011*, *Public Sector Act 2022*, the Code of Conduct for the Queensland Public Service, and the *Information Privacy Act 2009*.
- 5.1.3. This policy applies to the use of ICT services and devices whether on or off Queensland Health's premises. Staff may be disciplined (up to and including termination) for inappropriate or improper conduct in their official capacity or their private capacity if conduct adversely affects the public service.
- 5.1.4. Authorised users should not consider their activities, whether personal or business-related, conducted on Queensland Health's ICT services and devices as private. They may be accessed, used, or disclosed if required by or permitted under a law, including for example, in accordance with the *Right to Information Act 2009*.

## 5.2. Official use

5.2.1. Official use refers to use in an official capacity as a Queensland Health representative. Employees acting in an official capacity should disclose their position and indicate that they are representing Queensland Health, but must not disclose non-public information, commit Queensland Health to any action or engage in activities unless authorised to do so. Examples of official use may include, but are not limited to:

- using ICT services and devices for work related purposes
- using the internet to access work related information
- sending emails and instant messages to colleagues on work related matters
- sending emails outside of the work environment on work related matters, or
- updating departmental social media accounts, profiles or presence.

## 5.3. Professional use

5.3.1. Professional use is distinguished from official use. It refers to activity for professional development purposes, engaging with professional associations or in professional discussion forums, and networking with colleagues or peers.

5.3.2. Professional use generally occurs in non-work time or during work hours if authorised and should not interfere with official duties or affect productivity.

5.3.3. Professional use includes using ICT services and devices for education and self-development purposes, such as Study and Research Assistance Scheme or other approved study, research or professional forums.

5.3.4. Professional use allows employees in their private capacity to engage in conversation as an experienced person in their particular field and with other practitioners in that field.

5.3.5. All comments made in a professional capacity should be clearly attributed as personal views and not the views of Queensland Health and must not imply official endorsement or disclose non-public information, breach confidentiality or privacy obligations. Staff should avoid making comments that could be interpreted as official comment and may wish to include a disclaimer. For example, “This is my personal opinion and does not represent the opinion or position of the Queensland Government”.

5.3.6. Staff must be aware that any comment could compromise their perceived capacity to perform their official duties in an independent, professional, and unbiased manner. Staff should contact the relevant Communication and Media Branch for further information about making public comment.

## 5.4. Personal use

5.4.1. Limited personal use refers to activity conducted on Queensland Health ICT devices for purposes other than accomplishing official business or professional purposes that are consistent with departmental and HHS policy. Personal use of

ICT services and devices is permitted; however it is a privilege, not a right, and may be revoked at any time. Personal use of ICT services and devices is subject to the same requirements as official use and professional use. Personal use must be limited and reasonable, that is:

- brief, infrequent and not interfere with the operation of Queensland Health
- wherever possible, take place during non-work time (e.g., during breaks)
- lawful, ethical and efficient
- only incur negligible additional cost to Queensland Health.
- not embarrass or compromise the reputation of Queensland Health.

5.4.2. Staff accessing streaming services and other entertainment or social media sites for personal use must ensure that they do not connect through the Queensland Health network unless authorised to do so.

5.4.3. Managers considering approving access to these services for particular staff must follow the approved local access processes, consider the bandwidth of the facility and network limitations, and ensure conditions of use align with these processes and considerations and are clearly explained to, and agreed with, those staff.

5.4.4. Where facilities offer Staff Accommodation Filtered WiFi internet for personal use staff must do so in line with the Code of Conduct for Queensland Public Service, whole of government and Queensland Health policy and local directives.

5.4.5. Staff should consider security risks when using Queensland Health credentials (e.g. work email address) for non-work related purposes.

**Note:** All personal use of Queensland Health's ICT services and devices is at the user's risk. Queensland Health cannot guarantee the security of personal details that are transmitted using Health's ICT services and devices and is not liable for any loss or damage incurred by the user due to personal use.

## 6. Compliance

### 6.1. Non-compliance

6.1.1. Non-compliance with this policy represents a risk to Queensland Health's information, systems, or reputation. Failure to comply with this policy may result in:

- disciplinary action for breaching legislation, including, but not limited to:
  - *Criminal Code Act 1899*
  - Code of Conduct for the Queensland Public Service
  - *Financial Accountability Act 2009*
  - *Hospital and Health Boards Act 2011*
  - *Public Records Act 2002*
  - *Public Sector Act 2022*
  - *Information Privacy Act 2009*

- serious breaches may be referred to and investigated by the Queensland Police Service.

## 6.2. Reporting

6.2.1. All security breaches must be reported to the appropriate delegate or area and logged in the online IT portal for investigation as soon as possible. For more information contact your local Cyber Security area.

6.2.2. All privacy breaches or the misuse or suspected misuse of ICT services and devices, must be reported to the appropriate delegate or area for investigation as soon as possible.

## 7. Human rights

The policy 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.

## 8. 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).*

## 9. 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
  - Use of ICT services and devices standard
- Data and application custodianship policy
- Data and application custodianship standard
- Discipline HR Policy E10
- 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
- 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
- Records governance policy.

## 10. Definitions

Term	Definition
Authorised users	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.
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
Staff filtered accommodation WiFi	Delivers filtered internet for use by staff within the accommodation block. It provides standalone internet connectivity separate to the Queensland Health corporate network.

For further ICT definitions please refer to:

[Digital policy glossary](#)

## 11. Approval and implementation

Policy Custodian	Policy Contact Details	Approval Date	Approver
Deputy Director-General eHealth Queensland	<a href="mailto:Digital-policy@health.qld.gov.au">Digital-policy@health.qld.gov.au</a>	17/10/2024	Director General

## Version control

Version	Date	Comments
1.0	01/03/2021	New policy. Endorsed by Architecture and Standards Committee. Approved by Director-General.
2.0	17/10/2024	Cyclic review undertaken.

Version	Date	Comments
		See Change Table below.
		Endorsed IMSGC
		Endorsed ISC
		Endorsed ASC
		Approved Director-General.

## Change table

Section	Change
Statement	Statement updated For the purposes of this policy ICT services and devices includes, but is not limited to, <a href="#">computers</a> , <a href="#">laptops</a> , ICT network, ICT enabled medical devices, infrastructure, applications, portals, cloud, mobile devices, internet, storage, email, <a href="#">external access</a> , <a href="#">collaboration services</a> , Bring Your Own Device (BYOD), telecommunications, printers, faxes, photocopiers and video conferencing equipment.
Purpose	Dot point 3 updated <ul style="list-style-type: none"> <li>describe the access, <a href="#">use</a>, and <a href="#">auditing</a>, monitoring and record keeping requirements for ICT services and device</li> </ul>
Principles	New Principle added <b>Accountability and Responsibility:</b> Is in accordance with the Code of Conduct for the Queensland Public Service, public sector ethics and other applicable legislation
	New Principle added: <b>Respect for Human Rights:</b> Queensland Health is committed to upholding the principles embodied in the <i>Human Rights Act 2019</i> in all aspects of its ICT operations. This includes but is not limited to the rights to privacy, freedom of expression, and access to information. All ICT initiatives and practices are designed and implemented with due consideration for the protection and promotion of human rights as outlined in the Act.
Requirements	Legislation Reference updated <i>Public Service Act 2008</i> replaced with <i>Public Sector Act 2022</i> . Reference to National Privacy Principles removed.
5.1 Use of ICT services and devices	New requirement Authorised users should not consider their activities, whether personal or business-related, conducted on Queensland Health's ICT services and devices as private. They may be accessed, used, or disclosed if required by or permitted under a law, including for example, in accordance with the <i>Right to Information Act 2009</i> .



Section	Change
5.2 Professional use	<p>New requirement</p> <p>5.3.3. Professional use includes using ICT services and devices for education and self-development purposes, such as Study and Research Assistance Scheme or other approved study, research or professional forums.</p>
5.4 Personal use	<p>New requirements</p> <p>5.4.2. Staff accessing streaming services and other entertainment or social media sites for personal use must ensure that they do not connect through the Queensland Health network unless authorised to do so.</p> <p>5.4.3. Managers considering approving access to these services for particular staff must follow the approved local access processes, consider the bandwidth of the facility and network limitations, and ensure conditions of use align with these processes and considerations and are clearly explained to, and agreed with, those staff.</p> <p>5.4.4. Where facilities offer Staff Accommodation Filtered WiFi internet for personal use staff must do so in line with the Code of Conduct for Queensland Public Service, whole of government and Queensland Health policy and local directives.</p> <p>5.4.5. Staff should consider security risks when using Queensland Health credentials (e.g., work email address) for non-work related purposes.</p>
6. Non-compliance	<p>Added:</p> <ul style="list-style-type: none"> <li>• <i>Financial Accountability Act 2009</i></li> <li>• <i>Information Privacy Act 2009</i></li> <li>• <i>Public Records Act 2002</i></li> </ul>
6.2 Reporting	<p>New requirements</p> <p>6.2.1. All security breaches must be reported to the appropriate delegate or area and logged in the online IT portal for investigation as soon as possible. For more information contact your local Cyber Security area.</p> <p>6.2.2. All privacy breaches or the misuse or suspected misuse of ICT services and devices, must be reported to the appropriate delegate or area for investigation as soon as possible.</p>
7. Human Rights	<p>New requirement</p> <p>(Added to support the <i>Human Rights Act 2019</i>)</p> <p>The policy aligns with the <i>Human Rights Act 2019</i>, emphasising adherence to its principles. This ensures that our operations prioritise legal compliance and respect for individual rights.</p>