Use of ICT Services Policy

Use of ICT Services Implementation Standard

1. Purpose

This Implementation Standard outlines the responsibilities of authorised users and details the departmental responsibilities for managing and monitoring the use of Information and Communication Technology (ICT) services.

2. Scope

This Implementation Standard applies to all employees, contractors and consultants within the Department of Health divisions, agencies and commercialised business units.

This standard can be used by Hospital and Health Services either as is, by re-branding or as a base for a Hospital and Health Service specific standard.

The official use of social media is out of scope for this standard.

3. Supporting documents

Authorising Policy and Standard/s:
- Use of ICT Services Policy

Procedures, Guidelines and Protocols:
- Print Services Management Protocol
- Use and purchase of Mobile Phones Guideline
- Authorised and unauthorised use of ICT Services Guideline

4. Related documents

- Code of Conduct for the Queensland Public Service
- Queensland Government Enterprise Architecture, Department of Science, Information Technology, Innovation and the Arts (DSITIA)
  - Use of ICT Facilities and Devices Policy (IS38)
  - Authorised and Unauthorised Use of ICT Facilities and Devices Guideline

Users are accountable for their access and use of ICT services.

Authorised use is provided for official business, and limited and reasonable professional and personal use.

ICT services are actively managed and monitored.
5. Requirements

5.1 Authorised Users

5.1.1 All staff shall ensure that they are appropriately authorised prior to accessing and using departmental ICT services. Staff receiving such authorisation are considered to be Authorised Users.

5.1.2 Authorised Users shall access and use departmental ICT services for their intended purposes according to the Queensland Government Enterprise Architecture Use of ICT Facilities and Devices Policy (IS38), the Code of Conduct for the Queensland Public Service, legislation and departmental policy.

5.1.3 All Authorised Users shall agree to the Responsible use of the computer system conditions on login to the network and in so doing, acknowledge accountability for any use of departmental ICT services under their control; including internet access and email messages,and awareness that such use may be subject to audit, public scrutiny and/or disclosure.

Usage of departmental ICT services includes:
1. The use of privately owned devices connecting or attempting to connect to departmental ICT services from any location
2. All information transmitted or made available via departmental intranet and email services
3. The use of all types of communication and information devices used to access departmental network, internet and email services.

5.2. Authorised and Unauthorised Use

Authorised use of ICT services

5.2.1 When authorising access to departmental ICT services, managers and supervisors shall 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
4. Limited and reasonable personal use.

Note

- All personal use of departmental ICT services is at the user’s risk.
- The department cannot guarantee the security of personal details (e.g. credit card details or bank account details) that are transmitted using departmental ICT services.
- The department is not liable for any loss or damage caused by using departmental ICT services for personal use.

Unauthorised Use of ICT Services

5.2.2 All Authorised Users shall not use departmental ICT services for unauthorised or inappropriate purposes including (also refer to Unauthorised Use in definitions):

1. Propagating, transmitting, transferring, accessing, uploading, downloading or disseminating any communication in any form including text, images, sound, or direct links to such material in published hypertext documents, where the content and/or meaning of the material or its transmission or distribution is likely to be in breach of the Code of Conduct for the Queensland Public Service or legislation or departmental policy.
2. Enabling a person who is not an Authorised User to access departmental ICT services
3. Personal use exceeding the definition of limited personal use (see definitions).

On becoming aware of potential Unauthorised Use, managers/supervisors shall consider the nature of the potential breach and make a determination.

The following action may be taken:

1. Temporary or permanent removal of access
2. Disciplinary action up to and including termination of employment
3. Legal action and prosecution.

**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 an ICT service does not in itself imply that an Authorised User is permitted to access and use that service.
- Use of ICT services that constitutes suspected official misconduct shall be reported in accordance with Requirements for Reporting Official Misconduct HR Policy E9.

**Inadvertent or accidental access to inappropriate sites or emails**

5.2.3 An Authorised User who inadvertently or accidentally accesses unauthorised, inappropriate or offensive material using ICT services shall:

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

**Taking ICT devices off site**

5.2.4 Authorised Users shall obtain written authorisation prior to taking ICT devices off site for official or personal use, with the exception of portable computers (including mobile and handheld devices) and telephones (including mobiles and smart phones) assigned to a specific role or position.

**5.3 Managing ICT Services**

**Monitoring and Filtering**

5.3.1 The department shall protect the operation of the departmental network and ensure compliance with the Code of Conduct for the Queensland Public Service, legislation and departmental policy by monitoring and/or filtering all use of ICT services.

In determining potential breaches to this policy, details of Authorised Users’ actions on ICT services can be accessed and retrieved from monitoring records.

In conducting monitoring, ICT support personnel may:

1. access details of user actions
2. suspend connectivity and access to an ICT device without notice
3. wipe all data at any time without notice due to:
   - a breach of policy having been detected (suspension or wiping depending on circumstances)
   - a device having been reported lost or stolen (suspension or wiping depending on circumstances)
Managing Access

5.3.2 Supervisor/Managers shall ensure that Authorised Users’ access to services and to specific application systems is relevant to their current role.

6. Review

This Standard is due for review on: 1 July 2015

Date of Last Review: New standard

Supersedes: Use of Internet, email and other ICT facilities and devices policy

7. Business Area Contact

Strategy and Architecture Office, Planning, Engagement and Performance Directorate, Health Services Information Agency

8. Responsibilities

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibility</th>
<th>Audit criteria</th>
</tr>
</thead>
</table>
| Director - General              | • establishment of human resources delegations including the authority to investigate potential breaches and initiate disciplinary action  
• designating those areas that have a legitimate business reason to access information which otherwise may be prohibited by this policy  
• endorsing appropriate fundraising activities for which ICT services may be used | Delegations are established. Exceptions are approved. Fundraising activities are endorsed. |
| Chief Human Resource Officer    | • ensuring that the disciplinary process is in place in accordance with Human Resource policies  
• taking appropriate action regarding significant breaches of the Use of ICT Services Policy  
• ensuring the Use of ICT Services Policy is incorporated in education programs and relevant policies. | Disciplinary process established. Breaches are managed. Education programs and relevant policies include Use of ICT Services Policy requirements as necessary. |
| Chief Information Officer       | • approving the Use of ICT Services Policy  
• ensuring the appropriate infrastructure, applications, networks and security are implemented to support the Use of ICT Services Policy  
• ensuring the Use of ICT Services Policy is reviewed regularly as per the review schedule | ICT environment supports requirements of the Use of ICT Services Policy. Documents and reviewed regularly and approved. |
| Managers and supervisors        | • taking reasonable steps to educate employees on their responsibilities under this policy and the | Employees are aware of their responsibilities |

Effective From: 1 July 2013
Department of Health: Use of ICT Services Implementation Standard

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibility</th>
<th>Audit criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>consequences for non-compliance • monitoring employee use of departmental ICT services to ensure that it is appropriate • removing access in a timely manner when employees leave the department • reporting any breaches of this policy to HR and/or senior management as appropriate • taking appropriate action to address issues (including inadvertent or accidental access or non-compliance) • ensuring that access to services and to specific application systems are relevant to a user’s current role</td>
<td>under the Use of ICT Services Policy. Breaches are reported and issues are addressed.</td>
</tr>
<tr>
<td>Authorised Users</td>
<td>• complying with this policy; related departmental policies, standards and guidelines; the Code of Conduct for the Queensland Public Service and relevant legislation • ensuring any non-official use falls within the definitions of personal or professional use • immediately advising their supervisor/manager if they inadvertently or accidentally access unauthorised, inappropriate or offensive material using departmental ICT services</td>
<td>Completed appropriate training Notified supervisor/manager of any accidental misuse</td>
</tr>
</tbody>
</table>

9. Definitions of terms used in the policy and supporting documents

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition / Explanation / Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorised Use</td>
<td>Use by individuals who have received authorisation before operating the relevant device or service.</td>
<td>Queensland Government Enterprise Architecture (QGEA) Glossary</td>
</tr>
<tr>
<td>Authorised User</td>
<td>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. (See QGEA Authorised and unauthorised use of ICT facilities and devices guideline for further clarification).</td>
<td>QGEA Glossary</td>
</tr>
<tr>
<td>Disciplinary Action</td>
<td>Action taken as an outcome of a disciplinary process in accordance with the Public Service Act 2008.</td>
<td>Queensland Health Discipline HR Policy</td>
</tr>
<tr>
<td>ICT Facilities and Devices</td>
<td>ICT facilities and devices cover computers (including mobile and handheld devices); telephones (including mobiles and smart phones); 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; and fee-based web services. Queensland Health facilities and devices include ICT enabled medical</td>
<td>QGEA Glossary</td>
</tr>
<tr>
<td>Term</td>
<td>Definition / Explanation / Details</td>
<td>Source</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICT Services</td>
<td>ICT Services in the context of this policy and supporting documents refers to ICT Facilities and Devices as defined above.</td>
<td>QGEA Authorised and unauthorised use of ICT facilities and devices guideline</td>
</tr>
<tr>
<td>Official Use</td>
<td>Any use of the department’s ICT services for work-related purposes</td>
<td>QGEA Authorised and unauthorised use of ICT facilities and devices guideline</td>
</tr>
<tr>
<td>Personal Use</td>
<td>Activity conducted for purposes other than accomplishing official business or professional purposes that is consistent with departmental policy. Limited personal use of department-owned ICT services should be seen as a privilege and not as a right and is generally expected to: • take place during the employee’s non-work time (e.g. during an employee’s lunch break or after hours) and not be counted when accruing banked time or TOIL • incur minimal additional expense to the Queensland Government • be infrequent and brief, not delay official business and be for non-commercial purposes • not interfere with the operation of government and does not violate any state/departmental policy or related state/federal legislation and regulation. The Queensland Government accepts no liability for any loss or damage suffered by the employee as a result of personal use (for example internet banking).</td>
<td>QGEA Authorised and unauthorised use of ICT facilities and devices guideline</td>
</tr>
<tr>
<td>Professional Use</td>
<td>Activity for professional development purposes, engaging with professional associations or in professional discussion forums, and networking with colleagues or peers. Approval for professional use is at the discretion of senior officers, provided such use does not interfere with the activities of the department or affect the productivity of other employees and complies at all times with relevant department policy regarding acceptable behaviour.</td>
<td>QGEA Authorised and unauthorised use of ICT facilities and devices guideline</td>
</tr>
<tr>
<td>Spam</td>
<td>Unsolicited bulk e-mail or SMS messages which are generally of a commercial nature promoting or selling products or services. Often include illegal or offensive content and its purpose may be fraudulent.</td>
<td>QGEA Glossary</td>
</tr>
<tr>
<td>Unauthorised Use</td>
<td>Use of ICT Services that has not been authorised and includes use which is inappropriate, unlawful and/or criminal. Examples include but are not limited to the following list: • Uploading, downloading, storing, forwarding or in any way distributing or communicating unauthorised, unlawful, criminal, offensive or obscene material including - pornography - inappropriate pictures, graphics, jokes or messages (particularly any material of sexually explicit, racist sexist, discriminatory or otherwise potentially offensive behaviour, including the use of inflammatory, obscene, vulgar, insulting, abusive, threatening, harassing or provocative language) - unauthorised software</td>
<td>QGEA Authorised and unauthorised use of ICT facilities and devices guideline</td>
</tr>
</tbody>
</table>
Department of Health: Use of ICT Services Implementation Standard

Term | Definition / Explanation / Details | Source
---|---|---
- | Uploading, downloading, storing, forwarding or in any way distributing or communicating information that is untrue, defamatory, libellous, misleading or deceptive including impersonating or misrepresenting others |  
- | Conducting personal business for personal gain or profit or commercial purposes |  
- | Using ICT resources for  
  - Uploading or downloading inappropriate material such as malicious files of any kind, games, music, chain letters, etc. that affect productivity, may adversely impact the network and are not for officially approved purposes  
  - Accessing inappropriate services e.g. dating or gambling  
  - Creating and maintaining unapproved personal websites |  
- | Participation in external organisations including lobbying or political or religious advocacy |  
- | Uploading any personal information of third parties (including colleagues) without their prior consent |  
- | Providing third party information or material without obtaining the appropriate intellectual property permissions |  
- | Contributing to public discussion in an inappropriate manner including  
  - using work email address for personal comment  
  - disclosing or citing work related information without approval  
  - engaging in any attacks or insults including cyber bullying or cyber stalking  
  - engaging in any other action that could harm the goodwill or reputation of the department or the Queensland Government. |  

10. Approval and Implementation

Policy Custodian:
Executive Director
Planning, Engagement and Performance Directorate
Health Services Information Agency

Responsible Executive Team Member:
Ray Brown
Chief Information Officer
Health Services Information Agency

Approving Officer:
Ray Brown
Chief Information Officer
Health Services Information Agency

Effective From: 1 July 2013
**Approval date:** 31 May 2013  
**Effective from:** 1 July 2013

### Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Last Updated By</th>
<th>Last Review Date</th>
<th>Amendments/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>ICT Policy</td>
<td>29/04/2013</td>
<td>Finalised for approval.</td>
</tr>
<tr>
<td>1.1</td>
<td>ICT Policy</td>
<td>30/05/2014</td>
<td>Updated to include Print Services Management Protocol, current references and remove annual reporting requirement.</td>
</tr>
</tbody>
</table>