Use of ICT services

Standard

QH–IMP-032-1:2016

1. Statement

This 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.

All documents, messages, email and correspondence, whether official, professional or personal, that are created, sent, received or stored using Queensland Health's ICT services, information systems, facilities and devices remain at all times the property of Queensland Health and may be disclosed under mechanisms such as the Right to Information Act 2009 (Qld).

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

This standard should be read in conjunction with the Department of Health Information Security Standard.

2. Scope

Compliance with this standard is mandatory.

This standard applies to all employees, contractors and consultants within the Department of Health divisions and commercialised business units

3. Requirements

3.1 Requirements for authorised use

3.1.1 Authorised Users

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.

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.

All Authorised Users shall agree to the *Conditions of use* of the computer system 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.

3.2. Authorised and Unauthorised Use

3.2.1 Authorised use of ICT services

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.

3.2.2 Official, professional and limited personal use

Internet, email and other ICT services shall be provided to assist Authorised Users in the performance of their official duties, while allowing for professional and limited personal use.

In all cases, employees shall abide by legislative requirements including the Public Service Act 2008, the Code of Conduct for the Queensland Public Service and the National Privacy Principles in the Information Privacy Act 2009. Employees can be disciplined or dismissed for conduct considered inappropriate or improper in both their official capacity and their private capacity if conduct reflects seriously and adversely on the public service.

Official use

Official use refers to use in an official capacity as an agency representative. Employees acting in an official capacity should disclose their position and indicate that they are representing the agency, but must not disclose non-public information, commit the Department of 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 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.

Professional use

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. 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. Professional use generally occurs in non-work time or during authorised work hours and should not interfere with official duties or affect productivity. Examples of professional use may include, but are not limited to:

- using the Internet, email or social media for professional development, such as the Study and Research Assistance Scheme (SARAS) or other approved study or research activity. This may include accessing an educational institution's website to download assignment or course notes, or emailing assignments to academic institutions. Note that writing assignments should be done in non-work time unless a specific period of work time has been negotiated and approved within a SARAS agreement.
- use of other ICT services to support study, self-education or professional development.
- engaging with professional associations, participating in professional discussion within the area of expertise and knowledge, or maintaining professional networks of colleagues and peers. For example, using social networking sites such as LinkedIn for this purpose.

All comments made in a professional capacity should be clearly attributed as personal views and not the views of the Department of Health, and must not imply official endorsement or disclose non-public information, breach confidentiality or privacy obligations. Employees should avoid making comment 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".

Employees 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

Communication, Online Services, Marketing and Media Branch for further information about making public comment.

Limited Personal use

Limited personal use refers to activity conducted for purposes other than accomplishing official business or professional purposes that are consistent with departmental policy.

Personal use of ICT services is permitted, as defined in this guideline, however, it is a privilege not a right, and may be revoked at any time. Such use must be limited and reasonable, that is:

- be infrequent and brief in usage. As a guide, use that occurs more than a few times per day and/or for periods longer than a few minutes would not be considered limited personal use
- lawful, ethical and efficient
- wherever possible, take place during non-work time (e.g. during lunch breaks)
- only incur minimal additional cost to the Department of Health. Note: Where the private use component for a mobile, satellite or PDA telephone is more than the monthly specified amount in the user's terms and conditions, the total private use component is to be reimbursed to the Department of Health
- not impact on the Authorised User's productivity
- not be unauthorised as defined in this guideline
- not interfere with the operation of the agency, or contravene the Public Service Act 2008 or related State and Federal legislation and regulations
- not embarrass or compromise the reputation of the Department of Health.
- Personal use that conforms to the requirements outlined above and that would be considered limited and reasonable includes:
- family matters - arranging childcare matters, making appointments or installation/ service of utilities
- education - accessing an educational institution's website to download assignments or course notes; emailing assignments to academic institutions
- faxing, photocopying and printing – using ICT services to send small private documents, or copying or printing a few pages of personal information
- checking public transport timetables
- internet searching – limited personal internet searches that are not inappropriate, unlawful or criminal
- social networking – updating professional profile or using social media to keep in touch with friends and family, or news and current events
- banking/bill paying – arranging day-to-day activities such as paying bills and banking
- accessing Telstra White and Yellow Pages.

Social media for personal or professional use

Employees should not use their departmental email address when creating or accessing social networking accounts and should not use departmental or Queensland Government logos that may give the impression of official support or endorsement of personal comments made online.

When accessing social media using Department of Health ICT services users should:

- check account and privacy settings – understand who can access the account information and postings, and ensure more personal information is not revealed than is necessary.
- review posts – be mindful that content posted online is publicly accessible and will exist for a long time (even if deleted). Do not post anything that friends, family, colleagues or a manager should not see. Content posted can also be used as source material for journalists and other interested parties. As a general rule, think before posting on social media.
- consider any friend requests carefully – especially from people not personally known.

3.2.3 Unauthorised Use of ICT Services

All Authorised Users shall not use departmental ICT services for unauthorised or inappropriate purposes. The following examples of unauthorised use of ICT services are not intended to be exhaustive. Managers/supervisors should adopt a common sense approach and use reasonable judgement to assess each situation on its merits.

Unauthorised use of ICT services shall include but not be limited to:

- use by any person who is not an Authorised User
- enabling a person who is not an Authorised User to access ICT services
- use that is inconsistent with Queensland Government or departmental policies, guidelines or Code of Conduct for the Queensland Public Service
- operating a personal or not-for-profit business from work. For example, providing a work telephone, work mobile number or email address for this purpose
- fundraising, except for those endorsed by the Director-General or Chief Executives
- endorsing any product or service
- participating in any lobbying activity or engaging in political activity.
- faxing large, non-work related documents
- copying or printing large non-work related documents
- stealing data or intellectual property
- gaining or seeking to gain unauthorised access to other information systems, communication devices, facilities or entities
- soliciting money for religious or political causes, advocating religious or political opinions, or endorsing political candidates or parties
- capturing images with a departmental camera, including a camera in a departmental mobile telephone, hand held device or webcam, where content is likely to be considered pornographic, racist, discriminatory, inflammatory, defamatory, sexually explicit, obscene, abusive, threatening, harassing, offensive or likely to cause offence or be considered as socially unacceptable
- use of departmental television sets, DVDs, videos and cameras for personal use, unless prior authorisation has been received
- loading, installing and operating privately owned software, games, recreational software, screen savers, freeware / shareware, or non-work related software packages, with or without copyright licences.

Unauthorised use of internet facilities shall include:

- Propagating, transmitting, accessing, downloading, 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 considered:
  - pornographic
  - racist
  - discriminatory
  - inflammatory
  - defamatory
  - sexist
  - sexually explicit
  - obscene
  - abusive
  - threatening

  - offensive
  - harassing
  - likely to cause offence, or which would be considered socially unacceptable.
- knowingly accessing pornographic sites and disseminating, soliciting or storing sexually orientated messages or images
- excessive use for non-work purposes, even if conducted during non-work time
- accessing non-business related audio and video streaming or push technologies
- developing and maintaining a personal web page on or from departmental devices
- providing departmental or Queensland Government email addresses as part of contact details or a personal identifier on web sites or email lists not maintained by the Department of Health and/or Queensland Government unless such use is for work-related purposes or is consistent with personal use that is authorised by the department
- publishing comments or disclosing non-public information in online environments that have the potential to damage the department's reputation. Non-public departmental information includes information that is not available on the department's internet site or contained in reports
- creating, distributing or purposely activating any form of malicious software including, but not limited to, software generally known as computer viruses, worms or Trojans
- accessing peer-to-peer networks
- intentionally performing any act to knowingly degrade the performance of any system forming any part of the internet or departmental network facility
- distributing information for political purposes, except for the Minister's Office
- accessing internet sites dedicated to personals classified advertisements including dating, escort services or mail-order marriages
- accessing or playing real-time internet-based games, online gaming and gambling, chat rooms and messaging services and similar internet-based collaborative services. As these sites can cause congestion and disruption of networks or systems they are not to be accessed.

Unauthorised use of email facilities and instant messaging shall include:

- Propagating, transmitting, accessing, 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 considered:
  - pornographic
  - racist
  - discriminatory
  - inflammatory
  - defamatory
  - sexist
  - sexually explicit
  - obscene
  - abusive
  - threatening
  - offensive
  - harassing
  - likely to cause offence, or which would be considered socially unacceptable.
- Publishing or distributing:
  - material that purports to represent the official interests or opinions of the Department of Health other than in accordance with relevant departmental standards

  - personal information about any person without their prior authorisation including but not limited to, home telephone numbers, private addresses and information regarding the specific location of a person at any given time
- requesting the release of email messages blocked by filtering software where these messages are not for work purposes, because this involves a significant cost to the Department of Health
- mass posting the same inappropriate message to many newsgroups (spamming) or sending mass, unsolicited electronic mail
- distributing electronic 'chain letters', pyramid schemes or unsolicited advertising
- forwarding received emails that contain inappropriate images or text
- distributing recreational games
- distributing information associated with the activities, aims or objectives of a political party, group or individual
- operating personal or not-for-profit business(es) from work, including sale of personal property
- masquerading as any other person to send electronic mail messages
- using a generic or alias email address for personal or unauthorised use
- misrepresenting, obscuring, suppressing or replacing a user's identity on an email, including using false or misleading subject headers and presentation of information when distributing email for any unlawful, inappropriate, fraudulent or obscene purposes, or in support of such activities, including violation of copyrights or other contracts violating such matters as institutional or third party copyright, license agreements, and other contracts
- posting anonymous messages, or personal communications without the original author's consent.

Unauthorised use of telephone facilities shall include:

- calling information service providers for non-work-related business using premium, high cost services such as 1900 or 0055 prefixed numbers
- making International Dial Direct (IDD) calls for non-work purposes
- using mobile or satellite telephones by the driver of a vehicle whilst the vehicle is moving, or is stationary but not parked (unless using a personal or in-car hands free kit)
- making excessive personal telephone calls that impact on productivity
- taking inappropriate or pornographic pictures with photographic equipment, including mobile telephone cameras
- using mobile or satellite telephones in close proximity to fuel pumps or other sources of flammable fumes, or gases, or when they are likely to interfere with sensitive electronic/medical equipment.

3.2.4 Unauthorised use of information systems

All Authorised Users granted access to information systems have an obligation to ensure they only access information that is reasonably required for and consistent with the performance of their role and as approved by their line manager or supervisor.

Unauthorised use of information systems shall include but is not limited to:

- accessing, using or disclosing personal or health information when not directly related to duties or when accessing is not provided for under relevant legislation, for example:
  - Looking up health information for youself, a friend, family member, colleague or just out of curiosity
  - Talking to your friends about what you have read in a colleague's medical record
- accessing, using or disclosing personal, sensitive or confidential information when not directly related to duties or when accessing is not provided for under relevant legislation, for example:
  - viewing timesheets of other people in your team to check what leave they've taken and the hours worked when it is not part of your role to check and approve timesheets

- accessing or attempting to access information systems where access has not been granted, for example:
  - using (or trying to use) the log in ID and password for another team member
  - using the identity of another person to try and get access to information about them
- modifying information held in an information system when the modification is unauthorised, for example:
  - altering or deleting information for a colleague to remove any potentially damaging information

3.2.5 Unlawful use

- Unlawful use shall include, but not be limited to:
- 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 the Department of Health
- unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, copyright music, books or other copyrighted sources for which the Department of Health or the end user does not have an active licence is strictly prohibited
- exporting software, technical information, encryption software or technology, in violation of international or regional export control laws
- using mobile or satellite telephones when operating a vehicle whilst the vehicle is moving, or is stationary but not parked (unless using a personal or in-car hands free kit)
- 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
- sending messages without authority that may cause people to fear for their safety or the safety of other
- sending unsolicited commercial electronic messages (spamming)
- 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 (NPPs)
  - 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.*

Criminal use – violations of State and Federal law

Criminal use shall include, but not be limited to:

- accessing, downloading, on-forwarding, storing or distributing child pornography
- procuring or grooming persons under the age of consent for sexual purposes
- breaching copyright, for example by unlicensed copying of a computer program on a computer
- intercepting, accessing or altering data (hacking), or falsifying electronic documents or programs without legal authority to do so
- carrying out illegal activities (e.g. such as illegal gambling, fraud, stalking and unauthorised recording) or carrying out defamatory activities

- 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
- using any ICT facility or device to cause a 'denial of service' attack
- hacking into a computer system protected by a password or other security measure to access personal or commercial information or alter that information
- sending a threatening message such as a bomb threat
- accessing, transmitting or making available material that promotes suicide
- 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*.

On becoming aware of potential Unauthorised Use, managers/supervisors shall consider the nature of the potential breach and refer it to the appropriate HR Delegate to determine if further investigation is required.

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 the Department of Health's Discipline HR Policy E10
4. 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 corrupt conduct shall be reported in accordance with Requirements for Reporting Corrupt Conduct HR Policy E9.

3.2.6 Inadvertent or accidental access to inappropriate sites or emails

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.

3.2.7 Taking ICT devices off site

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.

3.3 Managing ICT Services

3.3.1 Monitoring and Filtering

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.

Monitoring of ICT services within the Queensland Health network shall be implemented using approved monitoring software, and shall be conducted only by authorised ICT support personnel or members of the Cyber Security Group, for the purposes of Network Protection duties.

Monitoring activities may require access to any information that is the property of Queensland Health including documents, messages, email or correspondence that is created, sent, received or stored by Authorised Users on Queensland Health ICT services, facilities and devices.

In monitoring to determine potential breaches to this policy, or security risks to the Queensland Health network, authorised ICT support or Cyber Security Group personnel may:

1. Access details of user actions and/or system activities including but not limited to:
   - addresses of internet sites visited
   - the number of incorrect password attempts
   - attempts by unauthorised persons to access Authorised User accounts or systems
   - systems and database/application logs
   - email activity in accordance with the *Employee Email Monitoring and Access Authorisation Standard*
   - actions or key events for accounts with privileged access.
2. Suspend connectivity and access to an ICT device and/or service 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)
   - disposal or transfer of the device to another authorised user (full wiping)
   - the device no longer being required to connect to departmental ICT services (suspension or wiping depending on circumstances).
4. Use the results of monitoring for the purposes of detecting breach of policy, malicious and/or suspicious activity, responding to security related events and alerts or for gathering forensic evidence in accordance with ICT incident management processes.

3.3.2 Managing access

Supervisor/Managers shall regularly review user access control lists to ensure that Authorised Users' access and account privileges to services and to specific application systems is relevant to their current role.

4. Recordkeeping and audit

All records and logs collected for the purposes of monitoring and security incident response and/or investigation shall be retained and be subject to audit in accordance with recordkeeping policy, including records that relate to the inspection of internet traffic for the purposes of detecting and/or remediating malicious or suspicious activity.

5. Related legislation and documents

Relevant legislation and associated documentation includes, but is not limited to, the following:

Legislation

- *Anti-Discrimination Act 1991*
- *Copyright Act 1968 (Cth)*
- *Crime and Corruption Act 2001*
- *Criminal Code Act 1899*
- *Cybercrime Act 2001 (Cth)*
- *Defamation Act 2005*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Hospital and Health Boards Act 2011*

- *Information Privacy Act 2009*
- *Privacy Act 1988 (Cth)*
- *Public Interest Disclosure Act 2010*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Telecommunications Interception Act 2009 (Cth)*
- *Right to Information Act 2009*
- *Spam Act 2003 (Cth)*
- *Work Health and Safety Act 2011*

Supporting documents

- Use of ICT ServicesPolicy
- Employee Email Monitoring and Access Authorisation Standard
- Bring Your Own Device (BYOD)Standard
- Print Services ManagementStandard
- Use and purchase of Mobile Phones Standard

Related policy or documents

- Code of Conduct for the Queensland Public Service
- Queensland Government Enterprise Architecture, Department of Science, Information Technology, Innovation (DSITI)
  - Use of ICT Facilities and Devices Policy (IS38)
  - Authorised and Unauthorised Use of ICT Facilities and Devices Guideline
  - Access and Use Policy (IS33)
  - Email monitoring and the Telecommunications (Interception and Access) Act guideline
  - Information Security Information Standard – IS18
  - Limited personal use of social media guideline
  - Recordkeeping Information Standard – IS40
  - Retention and Disposal of Public Records Information Standard – IS31
  - Queensland Government Use of Internet and Electronic Mail Policy and Principles Statement
- Officer of the Information Commissioner Queensland
  - Yammer. A private social network?
- Department of Health
  - Data Management Policy
  - Electronic Publishing Policy
  - Information Security Policy
  - Records Management for Administrative and Functional Records Policy
  - Clinical Records Management Policy
- Queensland Health
  - Discipline HR Policy E10
  - Financial Management Practice Manual
  - Requirements for Reporting Official Misconduct HR Policy E9
  - Union Encouragement HR Policy F4
  - Health Service Directive – Enterprise Architecture

6. Definitions

Term	Definition
Authorised Use	Use by individuals who have received authorisation before operating the relevant device or service.
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. (See QGEA Authorised and unauthorised use of ICT facilities and devices guideline for further clarification).
Confidential Information	Confidential information most often relates to patients of Queensland Health who may be living or deceased. Confidential information under the HHB Act means information, acquired by a person in the person's capacity as a designated person, from which a person who is receiving or has received a public sector health service could be identified.
Disciplinary Action	Action taken as an outcome of a disciplinary process in accordance with the *Public Service Act 2008*.
ICT Facilities and Devices	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 devices, satellite broadcasting and ICT enabled monitoring systems.
ICT Services	ICT Services in the context of this policy and supporting documents refers to ICT Facilities and Devices as defined above.
Information systems	The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.
Network Protection	Network Protection duties that are permitted under section 7(2) (aaa) of the *Telecommunications (Interception and Access) Act 2009 (Cth)* include duties relating to: (a) the operation, protection or maintenance of the network; or (b) ensuring that the network is appropriately used by employees, office holders or contractors of the agency or authority. Monitoring processes to protect the network include but are not limited to: • detecting breaches of policy • detecting malicious and/or suspicious activity e.g. intercepting and inspecting network communications • responding to security related events and alerts • gathering forensic evidence related to ICT incidents.
Official Use	Any use of the department's ICT services for work-related purposes
Personal information	Personal information is defined in the Information Privacy Act 2009 and can be any information or opinion about an identifiable living individual, including staff, patients and the community more broadly.
Personal Use	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

Term	Definition
	• 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).
Professional Use	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.
Sensitive Information	Sensitive information is a subset of personal information and it is important because of the heightened meaning or value to the individual concerned. Sensitive information is also defined in the Information Privacy Act 2009 and can include (but not limited to) any of the following: racial or ethnic origin; political opinions; religious beliefs, sexual preferences; criminal record; or health information.
Spam	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.
Unauthorised Use	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 • 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

Term	Definition
	- 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.

Version Control

Version	Date	Comments
1.0.	29 Apr. 2013	Approved for publishing
1.1	30 May 2014	Updated to include Print Services Management Protocol, current references and remove annual reporting requirement.
1.2	21 May 2015	Transferred to new template; mandatory clauses from guideline incorporated, reviewed by ICT Policy Unit.
1.3	19 January 2016	Minor amendment to current Standard
2.0	04 January 2017	Content reviewed. Approved CE eHealth Queensland