Office of the Information Commissioner
Queensland

POLICY - USE OF ICT SERVICES, FACILITIES AND DEVICES

1. Statement

The Office of the Information Commissioner (**OIC**) is committed to ensuring all use of OIC Information and Communication Technology services, facilities and devices (**ICT Services**) supports business activities for authorised purposes.

2. Scope

Compliance with this policy is mandatory. This policy applies to all users of OIC ICT services, including employees, students, contractors, and consultants.

Use of OIC ICT services include:

- OIC provided and/or privately-owned devices connected or attempting to connect to OIC ICT services from any location; and
- all information transmitted or made available via OIC intranet and email services.

3. Purpose

This policy supports consistent, authorised and lawful use of OIC ICT Services by requiring:

- ICT services are only used by Authorised Users for Authorised Use
- all staff understand their responsibilities when using OIC ICT services
- incidents of Unauthorised Use are logged, monitored, reported and managed appropriately
- ICT services are used in compliance with:
    - the OIC's policies, procedures, guidelines and staff training, the Code of Conduct for the Queensland Public Service; Queensland Government Enterprise Architecture (QGEA: Use of ICT Facilities and Devices Policy (IS38), Information Security Policy (IS18: 2018) and relevant State and Federal legislation.

4. Requirements

4.1 Authorised Users

All staff must be appropriately authorised before using OIC ICT Services. Staff who receive such authorisation from the Information Commissioner or delegate are Authorised Users.

All Authorised Users must agree to the Conditions of Use each time they access the OIC network. This includes acknowledging that they have read, understood and agree to this policy.

Authorised Users also acknowledge that all use may be subject to monitoring, audit, public scrutiny and/or disclosure, and that there are serious penalties for unauthorised use of OIC ICT Services, including, but not limited to, disciplinary proceedings and criminal prosecution.

4.2 Authorised use of ICT services

Authorised Users must only use OIC ICT services for an authorised use. Authorised use is limited to:

- official use
- professional use
- limited personal use.

Official use

Official use is use by an Authorised User in an official capacity. 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

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.

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.
- professional networking with colleagues and peers, provided this does not breach confidentiality or privacy obligations (e.g. maintaining an up-to-date profile on LinkedIn).

Limited Personal use

Limited personal use of OIC ICT services is a privilege, 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 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
- be able to survive public scrutiny and disclosure.

Note

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

Social media for personal or professional use

All staff need to be mindful of the way in which they engage via social media and the information they post. Employees should be aware that posting content that reflects seriously and adversely on the public service could give rise to disciplinary proceedings under the *Public Service Act 2008* (or applicable employing legislation).

All comments made in a personal capacity should be clearly attributed as personal views and not the views of the OIC. Users should avoid making comments that could be interpreted as official comment and may wish to include a disclaimer, however such a statement does not absolve the employee of the obligation to ensure their comments do not reflect seriously and adversely on the public sector, or the OIC as an independent integrity body.

Users should consult the QGCIO Personal use of social media guideline to understand their obligations when posting on social media. OIC staff should contact the Director, Engagement and Corporate Services, for further information about making public comment.

Should a staff member receive a message via a private social media account that constitutes official government business they should follow the Private email use policy.

4.3 Unauthorised Use of ICT Services

Authorised Users must not use OIC ICT services for unauthorised purposes.

Unauthorised use of ICT services includes, but is not 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
- gaining, or seeking to gain, unauthorised access to information systems, communication devices, facilities or entities
- use which is inappropriate, unlawful and/or criminal. Examples include, but

are not limited to:

- 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 behavior, 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, libelous, misleading or deceptive including impersonating or misrepresenting others
- Conducting personal business for personal gain or profit or commercial purposes
- 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 OIC or the Queensland Government.
- calling premium, high cost services such as 1900 or 0055 prefixed numbers and International Dial Direct (IDD) calls for non-work purposes
- making excessive personal telephone calls

Note

Authorised and Unauthorised Use conditions apply regardless of whether the use occurs within work hours or outside of work hours.

4.4 Unauthorised use of information systems

All Authorised Users granted access to information systems must only access information that is reasonably required for, and consistent with, the performance of their role and as approved by their manager or supervisor.

Unauthorised use of information systems includes, but is not limited to:

- accessing, using or disclosing personal, sensitive or confidential information when not directly related to your duties or when access, use or disclosure is not authorised under relevant legislation, for example:
  - looking up information for yourself, a friend, family member, or colleague, out of curiosity
  - talking to your friends about confidential information you have obtained in your role, such as non-public information about a high-profile applicant or complainant.

- 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 user
  - using the identity of another person to try and get access to information about them
- unauthorised modification of information held in an information system, for example:
  - altering or deleting information for a colleague to remove potentially damaging information

Note

The ability to connect to an OIC ICT service or information system does not in itself imply that a user is permitted to access and use that service.

Case study: Employee provided contact details for member of the public to colleague [1]

Facts
The offending behaviour took place in 2016 and involved a Senior Processing Officer accessing the TRAILS database at the request of a fellow employee (employee A) who had been involved in a road rage incident. The Senior Processing Officer gave employee A contact details for the other driver, which were used by employee A to abuse and threaten the driver on the telephone. The driver involved in the road rage incident made a complaint to the QPS regarding alleged threats made by employee A during the phone call.

Outcome
The department did not refer the conduct of the Senior Processing Officer who accessed the database to the QPS. The disciplinary outcome for the Senior Processing Officers was a pay point reduction for 12 months.

The disciplinary outcome for employee A was termination of employment.

Unauthorised use may attract penalties or constitute a criminal offence under relevant state and Commonwealth legislation including, for example, the *Criminal Code Act 1899*.

4.5 Reporting Unauthorised Use

On becoming aware of potential unauthorised use, managers/supervisors will consider the nature of the potential breach and immediately refer it to the appropriate delegate to determine if further investigation is required.

Use of ICT services that constitutes suspected unlawful use will be reported to the Information Commissioner. Allegations of unauthorised use may also be referred to the Queensland Police Service or Crime and Corruption Commission where appropriate.

Where unauthorised 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 sanctions and proceedings including termination, transfer, suspension, demotion in accordance with the *Public Service Act 2008*
4. Post-separation disciplinary proceedings.
5. Referral to appropriate law enforcement body.

Further information on assessing allegations of unauthorised use is provided in the Crime and Corruption Commission's Guide to Assessing Allegations about Misuse of Confidential Information.

[1] Crime and Corruption Commission (Qld). 2019. *Operation Impala - A report on misuse of confidential information in the Queensland public sector*, p.79. Accessed: https://www.ccc.qld.gov.au/publications/operation-impala-report-misuse-confidential-information-queensland-public-sector

4.6 Inadvertent or accidental access to inappropriate websites or emails

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

1. Not store or disseminate such material by whatever means
2. Delete such material including email messages immediately
3. Advise their supervisor/manager of the event as soon as practicable.

4.7 Taking ICT devices off site

Authorised Users shall obtain written authorisation prior to taking ICT devices off site for official, professional 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.

4.8 Managing ICT Services

Monitoring and Filtering

OIC logs and monitors all use of OIC ICT services in compliance with all relevant legislation, policies and procedures. Approved monitoring software is used and monitoring is conducted by authorised ICT support personnel for the purposes of Network and Systems Protection duties.

Monitoring activities may access any information that is the property of OIC. Documents, messages, email and correspondence created, received or stored using the OIC's services, facilities and devices are at all times the property of the OIC.

OIC will not seek individual or ad/hoc consent from OIC employees prior to any monitoring or inspection as a requirement to conduct either routine support and maintenance activities or executing formal investigative requests.

When undertaking monitoring activities, ICT support 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
    - 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.
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.

Managing access

Supervisor/Managers will 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.

5 Recordkeeping and audit

All records and logs collected for the purposes of monitoring and security incident response and/or investigation will be retained and subject to audit in accordance with obligations under the *Public Records Act 2002* (Qld) and the QGEA Records Governance Policy, including records that relate to the inspection of internet traffic for the purposes of detecting and/or remediating malicious or suspicious activity.

OIC will also retain records of training undertaken by staff on the use of ICT services, facilities and devices and employee agreements to comply with the OIC's policies and guidelines

6 Related legislation and documents

Relevant legislation and associated documentation include 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*
- *Defamation Act 2005*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Human Rights Act 2019*
- *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 and Access) Act 1979 (Cth)*
- *Telecommunications Interception Act 2009*
- *Right to Information Act 2009*
- *Spam Act 2003 (Cth)*
- *Work Health and Safety Act 2011*

Related policy or documents

- Public Service Commission
  - Use of the Internet and Email Policy
  - Private Email Use Policy
  - Code of Conduct for the Queensland Public Service.
- Queensland Government Enterprise Architecture, Department of Housing and Public Works (DHPW)
  - Use of ICT Facilities and Devices Policy (IS38),
  - Information Security Policy (IS18: 2018)
  - Authorised and Unauthorised Use of ICT Facilities and Devices Guideline
  - Information access and Use Policy (IS33)
  - Email monitoring and the Telecommunications (Interception and Access) Act guideline
  - Limited personal use of social media guideline
  - Records Governance Policy
- OIC
  - Human Resources Policies and Procedures
  - Financial Management Practice Manual
  - Bring your own device (BYOD) policy

7 Definitions

Term	Definition
Authorised Use	Use of OIC ICT services by Authorised Users, limited to: • Official use • Professional use • Limited personal use.
Authorised User	Users who have received authorisation to access OIC ICT services from the Information Commissioner (or delegate) and have agreed to abide by OIC policies, including the Use of ICT Services policy and the OIC Conditions of Use.
Confidential Information	Information including personal information, commercially sensitive information such as contracts or tender documents, and any other data, files or documents stored on an OIC device, network or database. Users must also observe the confidentiality requirements of the *Right to Information Act 2009* and the *Information Privacy Act 2009.*
Disciplinary Action	Action taken as an outcome of a disciplinary process in accordance with the *Public Service Act 2008*.
ICT Facilities and Devices	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; databases; internet; email; web mail; and fee-based web services. OIC facilities and devices include ICT enabled devices and ICT enabled 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 and Systems 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	Use in an official capacity by an Authorised User. 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 OIC social media accounts, profiles or presence.
Personal Information	Information or an opinion, including information or an 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 the information or opinion.
Personal Use	Authorised use of OIC ICT services for purposes other than Official Use or Professional Use that is consistent with OIC policy.
Professional Use	Activity for professional development purposes, engaging with professional associations or in professional discussion forums, and networking with colleagues or peers.
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 Disclosure	Unauthorised disclosure of confidential information, including personal information.
Unauthorised Use	Use of ICT Services, including use by Authorised Users, that is not authorised use. This can include use that is a violation of OIC policy, the Code of Conduct for the Queensland Public Service and relevant legislation.

Version Control

Version	Date	Comments
1.0	28 August 2020	Approved for publication