Use of ICT services, facilities and devices (IS38) implementation guideline

Final

November 2020

V2.0.3

OFFICIAL – Public

Document details

|  |  |
| --- | --- |
| 1. **Security classification**
 | 1. PUBLIC
 |
| 1. **Date of review of security classification**
 | 1. December 2015
 |
| 1. **Authority**
 | 1. Queensland Government Chief Information Officer
 |
| 1. **Author**
 | 1. Queensland Government Chief Information Office
 |
| 1. **Documentation status**
 |  | 1. Working draft
 |  | 1. Consultation release
 | 1. 🗹
 | 1. Final version
 |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office
qgcio@qgcio.qld.gov.au

Acknowledgements

This version of the *Use of ICT services, facilities and devices (IS38) implementation guideline* was developed and updated by Queensland Government Chief Information Office.

Feedback was also received from a number of departments, which was greatly appreciated.

Copyright

*Use of ICT services, facilities and devices (IS38) implementation guideline*

Copyright © The State of Queensland (Department of Science, Information Technology and Innovation) 2015

Licence



This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact qgcio@qgcio.qld.gov.au.

To attribute this material, cite the Queensland Government Chief Information Office.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Introduction 5](#_Toc57033337)

[1.1 Purpose 5](#_Toc57033338)

[1.2 Audience 5](#_Toc57033339)

[1.3 Scope 5](#_Toc57033340)

[1.4 QGEA domains 6](#_Toc57033341)

[2 Background 6](#_Toc57033342)

[2.1 Relationship to Public Service Commissions’ *Use of Internet and email policy* 7](#_Toc57033343)

[3 Departmental policies and practices 8](#_Toc57033344)

[4 Access to ICT services, facilities and devices 9](#_Toc57033345)

[4.1 BYOD and internet accessible services (including cloud) 9](#_Toc57033346)

[5 Authorised and unauthorised use 11](#_Toc57033347)

[5.1 Limited personal use 11](#_Toc57033348)

[6 Ownership of material 12](#_Toc57033349)

[7 Monitoring issues 12](#_Toc57033350)

[7.1 Monitoring policies 12](#_Toc57033351)

[7.2 Email monitoring and the TIA Act 14](#_Toc57033352)

[8 Incident management 14](#_Toc57033353)

[9 Audit and evidentiary records 15](#_Toc57033354)

[10 Disciplinary procedures 15](#_Toc57033355)

[11 Authorised investigations 16](#_Toc57033356)

[12 Unsolicited material 17](#_Toc57033357)

[13 Security 17](#_Toc57033358)

[14 Employee education and awareness 18](#_Toc57033359)

[14.1 Employee training and awareness programs 18](#_Toc57033360)

[14.2 Evidence of employee training 19](#_Toc57033361)

[14.3 Employee acknowledgement 20](#_Toc57033362)

[14.4 Other relevant information 21](#_Toc57033363)

[Appendix A Definitions 22](#_Toc57033364)

[Appendix B Related legislation and other requirements 23](#_Toc57033365)

[Appendix C Example headings – Use of ICT services, facilities and devices policy 24](#_Toc57033366)

[Appendix D Example process – receipt of inappropriate emails 27](#_Toc57033367)

[Appendix E Example of employee agreement on the use of the internet and email 28](#_Toc57033368)

# Introduction

## Purpose

This guideline provides information and advice for Queensland Government departments to consider when implementing the policy requirements of the [Use of ICT services, facilities and devices policy (IS38)](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2488-use-of-ict-facilities-and-devices-is38). This guideline does not form the mandatory component of IS38 and is for information only. While some information communicates other mandatory obligations which may be relevant in the context of IS38 (e.g. legislation), departments are strongly recommended to further investigate these obligations in light of their own business requirements, and seek legal/expert advice where necessary.

## Audience

This document is primarily intended for:

* chief information officers (CIOs)/other senior officers who authorise how departmental ICT services, facilities and devices may be used
* human resource professionals
* information management/ICT policy staff.

## Scope

### In scope

Employee personal use of government-provided ICT services, facilities and devices including where employee personal devices are used to access government email/Wi-Fi etc. is in scope.

### Out of scope

Employee use of personal services and devices for official purposes is outside the scope of this guideline and should be captured within departmental bring-your-own-device (BYOD) policies.

Official use of social media is outside the scope of this guideline and should be distinguished from limited personal use (including professional use) of social media via Queensland Government ICT services, facilities and devices. Official use of social media is any use of a Queensland Government-managed social media account, profile or presence by an authorised user. Comments made through official social media accounts are representative of the department and made by those authorised to do so. Uses can include: publishing messages, uploading content (text, images, video), and responding to communication from others. For further information, please refer to the QGEA *Principles of the Official use of social media networks and emerging social media* (link to be added once approved).

## QGEA domains

This guideline relates to the following domains:

|  |  |
| --- | --- |
| **Classification framework** | **Domains** |
| Business process | BP-2.4 Develop organisational regulationBP-8 Develop and manage human resourcesBP-9 Manage information and technology resourcesBP-11.6 Manage legislative obligationsBP-11.7 Manage legal and ethical issues |

# Background

ICT services, facilities and devices, including the internet and email are important sources of information and means of communication that can assist government to provide more effective services to the community.

The [Use of ICT services, facilities and devices (IS38) policy](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2488-use-of-ict-facilities-and-devices-is38) has been developed to provide departments with the minimum requirements when managing employee use of ICT services, facilities and devices. As stated within the IS38 policy, the provision of government-owned ICT services, facilities and devices are for officially approved purposes. Employee limited personal use of internet and email services, facilities and devices should be available on a basis approved by the department's chief executive officer. The use and/or access to these must be able to withstand public scrutiny and/or disclosure.

Employees are accountable to their employing department for the use of these technologies. Employees found to be intentionally accessing, downloading, storing or distributing pornography using government-owned ICT services, facilities and devices will, subject to industrial and procedural fairness, be dismissed.

Employees may also be subject to disciplinary action for the misuse of the internet or email in respect of material which is offensive or unlawful, although not pornographic. A pattern of behaviour (for example, repeated use) is a factor for consideration in determining disciplinary measures (including dismissal).

There are a number of other documents that support implementation of IS38. These documents are referred to throughout this document and also in figure 1 on page 7.



Figure 1: Use of ICT services, facilities and devices (IS38 suite of documents)

## Relationship to Public Service Commissions’ *Use of Internet and email policy*

The Public Service Commission’s (PSC) internet and email policy communicates the Queensland Government’s overarching policy principles in relation to the use of internet and email by employees. The policy applies to all Queensland public sector organisations and employees. One of the policy principles requires that all in scope agencies give specific consideration to IS38 and its guidelines when developing agency policy.

IS38 applies to Queensland Government departments only and requires departments to implement policies addressing employee use and monitoring of all ICT services, facilities and devices and ensure employee understanding of these policies. It is supported by detailed guidelines on employee use of ICT services, facilities and devices and monitoring.

In summary, the PSC’s *Internet and email policy* applies to a broader range of Queensland Government agencies. As the PSC policy refers to IS38, it in effect requires agencies within the applicability of the PSC policy but not IS38 to follow IS38. IS38 has a broader scope than the PSC policy, addressing the limited personal use of all government provided ICT services, facilities and devices. Whereas, the PSC policy focuses on limited personal internet and email use.

# Departmental policies and practices

1. Departments should develop and implement clear policies and practices for use of government-owned ICT services, facilities and devices. At a minimum, the policies should:
* reflect the needs of the business and be based on the risks associated with the particular service, device and/or facility
* state the types of [ICT services, facilities and devices](http://www.qgcio.qld.gov.au/products/glossary) and circumstances of use
* clearly state which [employees](http://www.qgcio.qld.gov.au/products/glossary) are covered under the policy, for example:

permanent, temporary, seconded staff

contractors or consultants

students, volunteers, work experience

other external bodies who are authorised by the department to use ICT services, facilities and devices.

* define which employees have access including employee conditions and constraints relating to their use of ICT services, facilities and devices in terms of security, privacy and delegations
* define what is considered authorised and unauthorised use, and the level and nature of such use
* include clear links to relevant legislative and policy obligations including the [Code of Conduct for the Queensland Public Service](https://www.qld.gov.au/gov/code-conduct-queensland-public-service), the [Public Service Act 2008](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) (Qld), [Public Sector Ethics Act 1994](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) (Qld), and the Public Service Commission’s - [Use of Internet and Email Policy](https://www.qld.gov.au/gov/documents/policy/use-internet-and-email-policy))
* address issues relating to recordkeeping [(Public Records Act 2002 (Qld))](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm), archiving, right to information, security, privacy [(Information Privacy Act 2009 (Qld))](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_I.htm) and audit requirements, noting that personal use of government-owned ICT services, facilities and devices may be subject to the *Right to Information Act 2009 (Qld)*
* address issues surrounding ownership of material
* inform employees of procedures that will be used to monitor compliance
* define disciplinary procedures and the consequences for breaches of the policy
* be reviewed on a regular basis (e.g. every two years)
* inform employees of their responsibilities and obligations regarding the use of ICT services, facilities and devices
* be readily accessible and regularly communicated to all employees.
* advise who employees can contact for further information
* advise on the relationship to any existing departmental bring-your-own device (BYOD) policies.
1. For definitions regarding types of ICT services, facilities and devices, and categories of employees refer to the QGCIO [glossary](http://www.qgcio.qld.gov.au/products/glossary).
2. To ensure clarity of these policies and guidelines departments should restate what resources can be used for private purposes and the limitations on the use of these devices in other departmental policies and documentation (e.g. terms of employment and/or information and systems access forms).
3. Departments may wish to develop one overarching policy for general use and responsibilities of ICT services, facilities and devices and then address significant areas in separate policy documents (for example, internet/email use and monitoring). However, this will be dependent on departmental documentation practices.

Example headings for use of ICT services, facilities and devices policy are provided at appendix B. However the following sections provide further information on issues to be considered as part of the department’s policies, guideline and/or supporting practices

# Access to ICT services, facilities and devices

1. As stated in the IS38 policy, departments may permit employees limited personal use of ICT services, facilities and devices. The level of this use needs to be in keeping with individual department policies and relevant legislation such as the [Public Sector Ethics Act 1994](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) (Qld) and [Public Service Act 2008](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) (Qld).

The policy should clearly define which employees within the department are authorised to use ICT services, facilities and devices, and the conditions and constraints relating to their use in terms of department security, privacy, copyright, confidentiality and delegation policies.

Departments are increasingly offering government provided ICT services to be accessed over the Internet through web browsers e.g. web-mail, remote file access and collaboration tools. These work services are often accessible to employees from personal equipment and networks. This means that these policies now apply to the ICT services, facilities and devices, not just inside the workplace, but also when used from locations outside the traditional workspace.

## BYOD and internet accessible services (including cloud)

1. ‘Bring Your Own Device’ (BYOD) continues to permeate into organisations and is a concept that is now expected by digital natives. Implementing BYOD within Queensland Government departments can help reduce hardware costs and increase productivity and flexibility. The ability to access meeting papers and notes from personal mobile phone devices for example also provides a convenient, efficient and environmentally friendly alternative to traditional methods. However, allowing the use of personal devices for official use within the workplace also creates a number of legal (e.g. privacy), financial recordkeeping and security risks that will need to be managed.
2. As the lines between personal and official use blur, departments should develop and implement BYOD policies. A risk based approach can be taken to balance the benefits of BYOD with the risks that it presents to ensure that a beneficial outcome is realised. The New South Wales Government has published a useful [BYOD Policy Toolkit](http://www.finance.nsw.gov.au/ict/priorities/infrastructure-and-managed-services/byod-policy-toolkit).

The implementation of a BYOD policy in culmination with the increasing number of internet accessible services in use or to be deployed within departments means there is improved access to work-related data without the need for significant amounts of data to be copied to personal devices.

Remote access and local access via BYOD should be considered as roughly equivalent. Depending on configuration differences in the nature and volume of access may arise resulting in increased scope for actual or perceived inappropriate use.

For instance, if a personal device is used and contains a copy of many sensitive records there may be little logging to defend against a claim of abusing access. Similarly, if a personal device is lost or stolen, the impact could vary significantly depending on what data is on the personal device.

When using BYOD staff are best protected by limiting replication of work information, especially sensitive and bulk information to personal devices.

Where replicating data to the personal device is warranted this should be done with work approval, for sound business reason and with appropriate security and risk awareness and ensure that the transfer of records to government recordkeeping systems and then delete such information off their devices once no longer needed.

Such approvals can be managed through processes to ensure that employees delete or transfer such information off their devices once no longer needed.

Ultimately, departments should ensure they communicate to employees how they can use both corporate supplied and personal devices and internet accessible services. Employees need to understand departmental policies and if in doubt not connect to departmental services until they have sought clarification.

Departments should also be aware of the Public Service Commission’s [Private Email Use Policy](https://www.forgov.qld.gov.au/documents/policy/private-email-use-policy) which provides specific direction with regard to messaging.

### Remote and BYOD access services management

When providing remote access and allowing BYOD access to work information and services, is important to maintain appropriate security and accountability for information access, sharing and protection. Staff with access must also be educated to make informed choices for both the information and devices they use.

For sensitive information and information of high value to criminals, consideration should be given to strong authentication and strong data controls e.g. two factor authentication and either thin client (no data to the device) or containerised (secure applications containers protecting the data when it gets to the device).

Internet accessible services are prone to being attacked, for these services application of access control policies become important to limit the scope of a successful attack against any one staff account.

Additionally, staff should ensure their personal devices used to access work information are well maintained so that they do not pose a high risk. Staff should also ensure that all work-related records received outside of official government accounts are transferred to a government business account. For further information see the Public Service Commission’s [Private Email Use Policy](https://www.forgov.qld.gov.au/documents/policy/private-email-use-policy).

Employees using their personal ICT services, facilities and devices can reduce their exposure to malicious web content (e.g. drive-by-downloads and viruses), hacking and identity theft by:

* maintaining up to date patching of the operating system and applications
* installing an active, regularly updated antivirus program
* being careful about what websites you visit and what you open, including being wary of clickbait (i.e. content aimed at generating advertising revenue, relying on sensationalist headlines to attract traffic)
* keeping device software up to date
* using strong passwords and two factor authentication mechanisms when available
* not use public computers to authenticate to any work account (e.g. login with username and password) as these are frequently targeted and credential capture is common
* not using wireless hotspots to access work services (excluding secure corporate ones) unless you have had confirmation from your information security team that the service is safe to use for your purpose
* using only trusted online payment websites
* being aware of the risks of phishing including scam emails for example promising huge rewards if you provide your bank account details
* minimising sharing of information such as date of birth, address, phone contacts, educational, and employment specific details (e.g. specific technical systems used in the workplace) on your social media profiles.

# Authorised and unauthorised use

1. It is of significant importance that departmental policy clearly defines what will be considered authorised and unauthorised use of departmental ICT services, facilities and devices. Departments need to clearly identify all uses for their circumstances and ensure that the information provided in these sections is clear and explicit, and provides comprehensive example of these uses.
2. When defining what is authorised and unauthorised use, departments need to carefully consider the core business of their department and the roles and responsibilities of their employees. It is recommended that departments use the headings ‘authorised use’ and ‘unauthorised use’ in their policies and guidelines in order to decrease associated legal risks. Departments need to ensure that use of departmental ICT services, facilities and devices is closely linked to business but strikes a balance between official and limited personal use.
3. Departments should ensure that practices are in place to ensure that employees are competent in the use of ICT services, facilities and devices. Access to these should be consistent with departmental security requirements and practices.

For further information refer to the [Authorised and unauthorised use of ICT services, facilities and devices guideline](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2739-authorised-and-unauthorised-use-of-ict-facilities).

## Limited personal use

In line with the Public Service Commission’s [Use of Internet and Email Policy](https://www.qld.gov.au/gov/documents/policy/use-internet-and-email-policy), department CEOs should determine the level and nature of personal use. Limited personal use is generally expected to take place during the employee's non-work time, incurs minimal additional expense to the government, is infrequent and brief, does not interfere with the operation of the government and does not violate any state/department policy or related State/Federal legislation and regulation.

1. When defining what constitutes limited personal use of ICT services, facilities and devices, departments should ensure that employees and regulatory bodies would perceive any restrictions to be sufficiently justifiable. Departments should ensure that where limited personal use is permitted (e.g. internet banking) that employees are aware that the government accepts no liability for any loss or damages suffered by the employee as a result of this personal use.
2. It is also recommended that the department’s policy should clearly outline:
* How is this to be authorised? For example, is access to the internet only after an employee has completed induction or some other form of training?
* What do they have access to? For example, is personal use of the internet only allowed to occur outside of business hours and incur minimal additional expense to the department?
* What are the conditions and constraints of such use, in relation to security, privacy, copyright, intellectual property, confidentiality and delegation?
* How will access be granted (passwords etc.)?

### Personal use of social media

The [Personal use of social media guideline](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2742-limited-personal-use-of-social-media-guideline) provides guidance on the limited personal use of social media via government provided ICT services, facilities and devices. In addition, the guideline provides helpful guidance when using social media via personal devices where use may impact on an employee’s public sector role.

# Ownership of material

1. Departments need to clearly communicate that documents, messages, email and correspondence created, received or stored using the department’s services, facilities and devices are at all times the property of the department.
2. As such this content may be accessed by authorised persons within the department at any time, and without any restriction. Staff should have no expectation of any right of privacy in relation to personal use of departmental ICT services, facilities and devices.

In addition departments should also highlight that any activity or information that employees generate as a result of their use of departmental ICT services, facilities and devices is not private and as such may be disclosed under mechanisms such as the [Right to Information Act 2009 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_R.htm).

# Monitoring issues

## Monitoring policies

1. Departments should ensure that their processes regarding the monitoring of ICT services, facilities and devices are clearly stated in the department’s policy. The extent of monitoring should be commensurate with the risk involved.
2. When developing monitoring policies and procedures, departments should:
* indicate that the use of ICT services, facilities and devices, may be monitored to identify any breaches of the department’s policy
* define what ICT services, facilities and devices may be monitored
* clearly identify under what conditions monitoring will occur including when monitoring of employee activity will occur
* define who has access to intercepted emails, monitoring reports and the delegation chain of authority and actions for dealing with reports or information collected or generated from this activity
* indicate what action will be taken if unauthorised activity is detected and that the department may in these circumstances also check the history of use of ICT services, facilities and devices by the employee
* detail monitoring practices which may include logs indicating internet sites employees have visited or billing charges for telephone services
* indicate which groups of employees are authorised to analyse:

logs that show use of ICT services, facilities and devices by employees or

content of employees' electronic files or email and to whom such authorised employees may disclose this confidential information about employees and for what purposes.

1. Departments should also ensure that processes are in place to address recordkeeping, archiving and right to information and audit requirements of ICT service, facility and device monitoring. As legislation takes precedence over the administratively based QGEA policies, departments will need to ascertain those laws which specifically relate to their activities in disclosing and using personal information.

To ensure the privacy of information sent to the department by a source outside of government, the department should ensure that they have clear policies and practices for dealing with information and reports generated from the interception of such emails.

The department should ensure it:

* expressly states the kinds of personal information that will be record in the course of intercepting incoming emails and the purposes for which the information will be used
* identifies who has access to intercepted emails and email monitoring reports
* defines the process for recording or dealing with personal information collected from this activity will be
* defines the delegation chain of authority and actions for dealing with reports or information collected will be.
1. Departments have a variety of methods and tools they can adopt to monitor employee use of ICT and enforce or encourage awareness and compliance with policy. These can be viewed under three broad groupings:
* Gateway and Network: These control and monitor traffic over the network, especially interactions to/from your department. Examples include filter web access including https proxies, email monitoring and enforced sensitivity marking, monitoring of other network traffic including intrusion detection and prevention systems.
* System: These control and monitor activities on individual servers and workstations. Examples include built-in system monitoring tools, tools that monitor actions of privileged accounts (perhaps including full key-logging), tools that detect or prevent installation and/or running of programs, tools that detect or prevent changes to system configuration, and hardware and software configuration controls such as monitoring or preventing use of devices such as USB.
* Application: These are typically features designed into applications that enable monitoring and control of user actions including actions that were prevented. Examples include application logs that capture actions of authorised users and other relevant data. For instance, an application that holds sensitive data may produce an audit trail of when sensitive data is accessed or attempted to be accessed and by whom.

## Email monitoring and the TIA Act

1. Departments should ensure that any monitoring of employees' internet use and interception of employees' email, including email originating from sources external to government, is undertaken in compliance with any relevant:
* Commonwealth legislation such as the [Telecommunications (Interception and Access) Act 1979 (Cth)](http://www.comlaw.gov.au/Details/C2013C00361), (the TIA Act), [Criminal Code Act 1995 (Cth)](http://www.comlaw.gov.au/Details/C2014C00676), [Cybercrime Act 2001 (Cth)](http://www.comlaw.gov.au/Details/C2004C01213)
* Queensland legislation such as the [Information Privacy Act 2009 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_I.htm).

# Incident management

1. When defining processes for the management of any misuse of ICT services, facilities and devices, departments should consider addressing the following issues:
* the process if employees discover unauthorised, unlawful or criminal use of ICT services, facilities and devices, informing them as to whom they can report such use
* the process for employees to report unintentional access or unsolicited emails that contain inappropriate material to managers or supervisors
* the process for dealing with incidents where employees receive inappropriate emails
* specifying the roles, responsibilities and procedures for investigating misuse of staff and management for example, the process for who monitors, how often, who decides what is appropriate or not and what needs to be escalated and who escalates it
* identifying the authority for commencing any disciplinary process and the delegation chain of authority to be followed.

An example process for the ‘Receipt of inappropriate emails’ is located in Appendix D. Departments should also refer [Information security (IS18)](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy) and the suite of supporting documents relating to incident management when implementing and documenting incident management processes to ensure alignment with existing departmental security policy.

# Audit and evidentiary records

1. Departments should ensure that processes and policies are in place to maintain appropriate records resulting from misuse of ICT services, facilities and devices, these should include:
* establishing a process to identify an audit trail for identification of misuse
* data collection policies and procedures (in accordance with [Information Privacy Act 2009 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_I.htm), and compliance in principle with the [Criminal Code Act 1995 (Cth)](https://www.comlaw.gov.au/Details/C2015C00368)
* maintaining appropriate record keeping systems to comply with obligations under the [Public Records Act 2002 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm), [Recordkeeping (IS40)](https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2357-recordkeeping-is40), [Information Standard 31: Retention and disposal of public records](http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2360-retention-and-disposal-of-public-records-is31) and to assist with any RTI requests
* maintaining records that verify evidentiary requirements such as:

training undertaken by staff on the use of ICT services, facilities and devices

employee agreements to comply with the department’s policies and guidelines.

Further details on maintaining audit logs and recordkeeping requirements can be found in [IS18](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy) and [IS40](https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2357-recordkeeping-is40).

# Disciplinary procedures

1. When addressing issues relating to disciplinary procedures for misuse of ICT services, facilities and devices, departments should:
* define the range of disciplinary procedures and penalties which may be applied as a consequence of unauthorised use of internet and email including that the disciplinary action in the case of an employee being found to have intentionally accessed, downloaded, stored or distributed pornography using government-owned ICT services, facilities and devices is subject to industrial and procedural fairness, termination of employment
* ensure that the disciplinary action for intentionally accessing, downloading, storing or distributing pornography is communicated to all employees in clear and unambiguous language
* indicate the process to be followed and consequences for employees using internet and email services, facilities in an unauthorised way
* outline procedures for incident investigation and the responsibilities of staff and management in the disciplinary process
* ensure that incident reporting policies and processes include an escalation process for unlawful or criminal misuse
* ensure these processes generally reflect the same processes outlined in security incident reporting
* ensure decisions to involve law enforcement departments or the Crime and Corruption Commission are determined by the CEO (or delegate)
* indicate that employees have a right of appeal in relation to a department undertaking disciplinary action
* clearly identify the process to be undertaken to deal with unlawful or criminal use of ICT services, facilities and devices and that the appropriate authorities may need to be involved
* ensure that employees are aware of both the technical and content restrictions of sending and receiving email.
1. The course and extent of disciplinary action to be undertaken for the breach of departmental policy should be determined by the CEO (or delegate) on a case-by-case basis and should reflect the severity of the breach.
2. Departments should ensure that disciplinary procedures and penalties imposed on employees for breaches of use are clear, unambiguous and proportionate to the offence and are applied in a manner which is timely, fair and decisive. A pattern of behaviour (for example, repeated use) is a factor for consideration in determining disciplinary measures (including dismissal).
3. Departments should ensure that any breaches discovered are thoroughly investigated and all issues identified and addressed. It is of the importance that departments maintain up to date records of employee training which can be used as evidence during the investigation of unauthorised use. For further information other training tools and what type of information should be captured please refer to refer to section [14.2 Evidence of employee training](#_Evidence_of_employee).

Departments should indicate in their policies that employees have a right of appeal in relation to a department undertaking disciplinary action. Departments should also ensure that all cases of misuse are managed with industrial and procedural fairness. Possible penalties arising from disciplinary action in addition to those set out in section 188 of the [Public Service Act 2008 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) may include penalties such as:

* revocation of authorised access to ICT services, facilities and devices
* revoking of use for a period of time.

Refer to the [Public Service Commission’s Chief Executive Guideline 01/13: Discipline guideline](https://www.qld.gov.au/gov/documents/guideline/discipline-guideline) for further information and guidance in relation to the management of potential disciplinary matters. Further information about the [Public Sector Ethics Act 1994](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) and the Code of Conduct for the Queensland Public Service can be obtained from the [Ethics in the Queensland Public Sector](http://www.ethics.qld.gov.au/) website.

# Authorised investigations

1. Departments should ensure that the department delegation and authorisation policies and procedures clearly address the authorisation of employees, who in the course of their duties, are required by the department, to access, download or store pornography for investigation purposes.
2. The roles and responsibilities for investigating misuse will vary across departments; ideally these responsibilities should be delegated to senior staff. In addressing this issue departments should consider implementing written agreements and/or clear role descriptions for employees involved in these activities to clearly detail the circumstances and processes under which investigations are to be conducted.

# Unsolicited material

1. As outlined in the Cabinet endorsed [Use of Internet and Email Policy](https://www.qld.gov.au/gov/documents/policy/use-internet-and-email-policy), departments should include in their policies that employees receiving inappropriate material from the internet or through an email should delete such material from departmental systems immediately and notify their supervisor/manager of their actions.
2. Such an action should not constitute unauthorised use. However, storage or dissemination of inappropriate or unacceptable material by whatever means constitutes unauthorised use. Deleting unsolicited emails not relating to the business of the department does not constitute unauthorised disposal under the [Public Records Act 2002 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm).
3. All cases of misuse should be considered on a case-by-case basis and the department should ensure that procedural fairness is applied in all cases. When investigating instances of unauthorised internet and email use, and whether such use was intentional or unintentional, departments may wish to consider the following factors:
* Did the employee delete the material from departments systems?
* Did the employee report the incident to their manager or supervisor?
* Did the employee advise the sender by email not to send further inappropriate emails or report the receipt of the inappropriate email/s to the departmental IT unit?
* How much time did the employee spend on the site?
* What is the employee's history of accessing inappropriate sites?
1. Department policies should also ensure that processes are in place and communicated to employees regarding the process for employees to report unintentional access or un-solicited emails that contain inappropriate material to managers or supervisors.
2. In 2003 the Federal Government passed the [Spam Act 2003 (Cth)](http://www.comlaw.gov.au/Details/C2014C00214), which provides standards for commercial electronic messages including those sent by Government. The [Spam Act 2003 (Cth)](http://www.comlaw.gov.au/Details/C2014C00214) says that unsolicited commercial electronic messages must not be sent. A message should only be sent to an addressee when that person has consented to receive it. The Act does provide some exemptions for government bodies, however these are limited.

For further information on refer to the Australian Communications and Media Authority’s [Spam Act 2003: A practical guide for government](http://www.acma.gov.au/webwr/consumer_info/spam/spam_act_pracguide_govt.pdf) to ensure that the provisions of the Act are addressed in departmental policies.

# Security

1. To address a wide range of security issues particularly in relation to internet and email, departments should refer to the [QGEA information security resources](https://www.qgcio.qld.gov.au/products/information-security) when implementing and documenting security systems and processes for the monitoring and access of ICT services, facilities and devices.
2. Whilst departmental security policies and processes give consideration to IS18, and deal with the majority of risk posed by internet and email use, departments should minimise security risks including disruption to the departments operations and unauthorised use (intentional or unintentional) by employees. Departmental use of ICT services, facilities and devices policies should also highlight specific issues including:
* information classification and control, for example the classification of information which can be circulated through internal email will vary considerably from the information that can be circulated through internet mail
* operational and access control security management, for example prohibiting connection of unauthorised portable ICT storage devices; firewall policies; the importance of passwords; remote access polices and external access to webmail
* the importance of virus protection
* use of mobile technology
* incident reporting and escalation including incident response management
* the procedures to minimise unsolicited and inappropriate emails (in accordance with the [Spam Act 2003 (Cth)](http://www.comlaw.gov.au/Details/C2014C00214))
* how data on employees’ use of the internet and email be collected and stored.
1. Many issues should already be dealt with in terms of department security policies, however to ensure staff are fully aware of the restrictions they should be reiterated in the policy with regards to internet and email use. For example:
* What are the limits on the size of mailboxes?
* What types of attachments will be limited in both incoming and outgoing emails?
* What is the protocol for sending email to broadcast groups or multiple external recipients?
* What is the department’s policy on encryption?
* What is the classification policy for sending information by email?
* What is the policy on downloads and viruses?
* Is the use of signature blocks mandatory for all outgoing email?
* What is the standard notifications to be included on outgoing email e.g., legal and confidentiality and copyright disclaimers?
* What emails need to be kept for records management purposes?
* What is the protocol for mailboxes of staff on leave?
* Is there a protocol or limit to the type and number of internet subscription lists?
* What is the department’s policy on downloading of software from the internet and how will this be managed?
* What is the department’s policy on fees for online information and how will this be managed?

# Employee education and awareness

1. Communicating policies and guidelines to employees is critical to the successful implementation and operation of the policy and the management of ICT services, facilities and devices across government. Departments need to determine when, how often and by what means this communication will occur.

The processes for regularly communicating all relevant policies and guidelines may take the form of notifying staff via email, newsletter distributed to all employees, briefing sessions, awareness programs, network log-on notices or on-line or face-to-face training.

## Employee training and awareness programs

1. Departments need to ensure all employees are aware of, understand, acknowledge and have access to the relevant departmental policies on the use of ICT services, facilities and devices including internet and email, and their responsibilities as outlined in the Public Service Commission’s [Use of Internet and Email Policy](https://www.qld.gov.au/gov/documents/policy/use-internet-and-email-policy) on an ongoing basis. This may be through employee induction processes and ongoing training.
2. Departments should define the processes they will use to ensure that all employees are aware of and acknowledge their responsibilities when using ICT services, facilities and devices. Issues that need to be considered include, the mechanisms that will be used to ensure access to policies by all employees including when, how often and by what means these policies will be communicated.
3. In addition, employee awareness of monitoring is very important. As ICT services, facilities and devices are government owned resources, the department has both a right and a public obligation to monitor them to ensure that they are not used wastefully or inappropriately. Departments should consider regularly communicate to employees that their use may be monitored, and the processes that will be used to monitor, audit and report on employee use and/or access. Communication to employees can act as a useful deterrent; even if departments only have resources to conduct periodic spot check monitoring. As an example, departments may wish to send an alert out to their employees which states:
4. “*Did you know that over the past 12 months, [xx no. of] employees were disciplined or dismissed for unauthorised use of ICT services, facilities and devices? For further information on your responsibilities when using the department’s ICT services, facilities and devices please refer to the [link to relevant department documents] or contact the [provide department contact details].*”
5. Departments should ensure employees are aware that:
* information created, received an stored on departmental ICT services, facilities and devices is the property of that department
* no activities they conduct on departmental ICT services, facilities and devices is private
* as such that information whether personal or business-related, may be disclosed under mechanisms such as the [Right to Information Act 2009](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_R.htm) (Qld).
* not just creating, but forwarding unauthorised emails can also be grounds for discipline or dismissal, so even if the sender was not the originator, the fact that an unauthorised email is being forwarded is enough for a department start an investigation.
1. Departments should ensure that training, education and communication of authorised usage policies are carried out on a regular basis. Methods for this training and awareness could include:
* code of conduct, acceptable usage policy updates and security ‘refresher’ training or briefing sessions
* notification of staff via email
* newsletters distributed to all employees, briefing sessions on employee responsibilities.

## Evidence of employee training

1. Departments should also consider how they will address training of employees in the use of ICT services, facilities and devices including:
* What training will be provided to employees in the use of internet and email?
* What records will be kept of employee training? (e.g. maintaining a register of when employees undertook training for recordkeeping and evidentiary collection purposes)
* How will these be maintained?
* How will employees acknowledge that they have read and understood the department’s policy?
* How will employees acknowledge they have read and understood the policy and Cabinet Statement on the use of internet and email?
* How will employees acknowledge that they understand that their internet and email use may be monitored?
* How will the department ensure that employees know that when receiving unsolicited inappropriate material from the internet or through an email, they delete such material from departmental systems?
* How will departments communicate employee responsibilities on the use of internet and email?
1. As mentioned previously, it is important that departments maintain up to date records of employee training which can be used as evidence during any investigations of unauthorised use. Training records, at a minimum, should capture information such as:
* training topic
* name of the instructor
* the date
* length of the training course
* trainee’s name.

Departments should consider the use of training sign-in sheets, which can be used as evidence in the event of a dispute. Training quizzes can also be an effective mechanism to support that an employee not only attended, but understood the content. Departments should also consider keeping a register of other employee communications such as email notifications, alerts and newsletters etc.

It is also important that all training records are kept up to date and revised following each training session.

## Employee acknowledgement

1. To ensure employees have an understanding of, and acknowledge their obligations and responsibilities when using ICT services, facilities and devices, departments may wish to consider the implementation of formal employee acknowledgement/agreements through written agreements.
2. To highlight the department’s policy on the use of ICT services, facilities and devices departments should consider inclusion of what resources (i.e. mobile phone, laptop computers etc.) can be used for private purposes and the limitations on the use of these devices in other departmental policies and documentation such as terms of employment and/or information and systems access forms. Issues to consider when defining policy and practices for this include:
* How will employees acknowledge they have read and understood the policy and Cabinet Statement on the use of internet and email? An example ‘Employee agreement on use of internet and email’ template is located at appendix E.
* How will employees acknowledge what is authorised and unauthorised use?
* How will the department ensure that employees know that when receiving unsolicited or inappropriate material from the internet or through an email, they delete such material from departmental systems immediately? (Action to delete this material would not constitute unauthorised use.)
* How will employees acknowledge their ethical and code of conduct obligation to report any improper conduct or practices of which they become aware?

Relevant departments should also be aware of requirements under the [Employment Separation Procedures Directive 15/14](https://www.qld.gov.au/gov/documents/directive/1514/employment-separation-procedures), issued by the Public Service Commission, to have procedures in place when an employee separates from employment in the Queensland public service. Departments should also ensure that these procedures are communicated to employees.

## Other relevant information

1. In addition to specific departmental policies and procedures on the use of ICT services, facilities and devices, departments should also ensure that they inform employees where they can freely access all other relevant information including:
* workplace health and safety and appropriate use of ICT services, facilities and devices e.g. this may include information on how to use adjustable workstations or 'in car' mobile phone headsets
* the penalties which apply to unlawful and criminal use of ICT services, facilities and devices
* the consequences of forwarding of chain letters or mass mailing of unsolicited junk mail (spam), or the downloading of data or programs that may strain system resources
* the potential for downloading viruses, worms, Trojan horses and spyware through email, files and attachments
* obligations on capturing, creating and disposing of emails, instant message etc. under the [Public Records Act 2002](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm) (Qld), [Information Standard 40: Recordkeeping](http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2357-recordkeeping-is40) and [Information Standard 31: Retention and disposal of public records](http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2360-retention-and-disposal-of-public-records-is31)
* departmental security policies in relation to information security classification schemes.
1. Definitions

The following definitions apply for the IS38 policy:

* [Employees](https://www.qgcio.qld.gov.au/products/glossary)
* [Government provided ICT, services, facilities and devices](https://www.qgcio.qld.gov.au/products/glossary).

Related legislation and other requirements

This appendix provides a summary of some of the related obligations that apply to Queensland Government departments. The contents of this appendix do not constitute legal advice and should not be relied on as a comprehensive statement of legislative and statutory obligations.

Queensland legislation

* [Anti-Discrimination Act 1991 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_A.htm)
* [Crime and Corruption Act 2001 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_C.htm)
* [Financial and Performance Management Standard 2009 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_F.htm)
* [Information Privacy Act 2009 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_I.htm)
* [Public Records Act 2002 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm)
* [Public Sector Ethics Act 1994 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm)
* [Public Service Act 2008 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_P.htm)
* [Right to Information Act 2009 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_R.htm)
* [Work Health and Safety Act 2011 (Qld)](https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_W.htm)

Commonwealth legislation

* [Copyright Act 1968 (Cth)](https://www.comlaw.gov.au/Series/C1968A00063)
* [Criminal Code Act 1995 (Cth)](https://www.comlaw.gov.au/Series/C2004A04868)
* [Cybercrime Act 2001 (Cth)](https://www.comlaw.gov.au/Series/C2004A00937)
* [Privacy Act 1988 (Cth)](https://www.comlaw.gov.au/Series/C2004A03712)
* [Spam Act 2003](https://www.comlaw.gov.au/Series/C2004A01214)
* [Telecommunications (Interception and Access) Act 1979](https://www.comlaw.gov.au/Series/C2004A02124/Compilations)

QGEA requirements

* [Use of ICT services, facilities and devices policy (IS38)](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2488-use-of-ict-facilities-and-devices-is38)
* [Authorised and unauthorised use of ICT services, facilities and devices guideline](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2739-authorised-and-unauthorised-use-of-ict-facilities)
* [Personal use of social media guideline](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2742-limited-personal-use-of-social-media-guideline)
* [Principles for the official use of social media networks and emerging social media](http://www.qgcio.qld.gov.au/products/qgea-documents)
* [Information standard 18: Information security (IS18)](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy)
* [Information standard 40: Recordkeeping (IS40)](http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2357-recordkeeping-is40)
* [Information Standard 31: Retention and disposal of public records](http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2360-retention-and-disposal-of-public-records-is31).

Other resources

* The Public Service Commission’s [Use of Internet and Email Policy](https://www.qld.gov.au/gov/documents/policy/use-internet-and-email-policy)
* The Public Service Commission’s [Code of Conduct](https://www.qld.gov.au/gov/code-conduct-queensland-public-service)
* The Public Service Commission [Directives](https://www.qld.gov.au/gov/directives-policies-and-guidelines)
* The Crime and Corruption Commission’s [Reporting Corruption](http://www.ccc.qld.gov.au/corruption/report-corruption)
* [Ethics in the Queensland Public Sector](http://www.ethics.qld.gov.au/) website
* Australian Communications and Media Authority’s [Spam Act 2003: A practical guide for government](http://www.acma.gov.au/webwr/consumer_info/spam/spam_act_pracguide_govt.pdf)[AS/NZS:38500:2010 Corporate governance of information technology](http://infostore.saiglobal.com/store/Details.aspx?ProductID=1390488).

Example headings – Use of ICT services, facilities and devices policy

Policy statement

[*The policy statement should be a concise statement of “what” the policy is intended to accomplish. It should clearly reflect the overall government direction, the department’s direction and what the policy is hoping to achieve, including alignment with the Cabinet endorsed Policy & Principles Statement and approved Code of Conduct. This section should contain a general statement emphasising the effective use of these devices (including the internet and email) as business, communication and education tools*]

Policy statement

[*States the department’s overall policy in the use of ICT services, facilities and devices and aligns with IS38, Cabinet endorsed Policy and Principles Statement and approved Code of Conduct*].

Applicability

[*Clearly states the employees that are covered under the policy, for example:*

* *permanent, temporary or seconded employees as defined by the Public Service Act 2008 (Qld)*
* *contractors (which should also be reflected in contract conditions)*
* *students*
* *volunteers*
* *work experience*
* *other external bodies as authorised by the department]*

Scope

[*Clearly states which ICT services, facilities and devices are covered under the policy, for example:*

* *computers, including palm, handheld and iOS technologies)*
* *telephones (including mobiles)*
* *removable media*
* *digital or analogue recorders (including DVD and video, cameras*
* *photocopiers, facsimile machines*
* *printers, scanners*
* *the internet, internal email, webmail and fee-based web services]*

Objectives

[*This section details the department’s policy objectives, how these policy objectives will be achieved. For example the department’s objectives could be to:*

* *establish a framework to manage employee use of ICT services, facilities and devices*
* *protect the department’s information assets through reducing the risk of unauthorised use*
* *establish effective governance arrangements including accountability and responsibility for employee use of ICT services, facilities and devices within the department*
* *maintain an appropriate level of employee awareness to minimise the occurrence of unauthorised use]*

Legal requirements

[*Outlines the relevant legal and statutory compliance requirements*].

Policy implementation

[*Details how the policy will be implemented including what resourcing will be supplied to support implementation and how the policy will be communicated and be accessible to all appropriate department employees. Details the performance measures or review mechanisms established to ensure the policy is being implemented effectively*].

Policy owner/enquiries

[*Identifies the owner of the policy and who is responsible for its development and ongoing review. Contact details for enquiries should be listed in this section*].

Policy approval and review

[*Provides details of who approved the department’s policy and the date of approval*].

Policy review

[*Provides details of when the policy will next be reviewed. Specifically it should indicate that periodic assessment and reviews of the policy will be undertaken to continue to address any risks associated with the use of ICT services, facilities and devices. For example, departmental Information Steering Committee or Risk Management Committee may schedule periodic reviews and assessments.*]

Security

[*This section should refer to the department’s security policies which specifically relate to the use of ICT services, facilities and devices and highlights specific issues, e.g., information classification and control. Internet and email restrictions should also be reiterated, e.g., mailbox size limits*]

Access to ICT services, facilities and devices

[*Clearly defines issues surrounding access to the department’s ICT services facilities and devices including who has access to what. Also include any linkages to existing departmental BYOD policies.*]

Authorised and unauthorised use

[*Clearly articulate what activities will be considered authorised and unauthorised, including examples of such activities*]

Internet and email use

[*Covers etiquette and best practice for Internet and email use. Should include social media including work collaboration tools such as Yammer..*]

Ownership of material

[*Outlines that documents, messages, email and correspondence created, received or stored using the department’s ICT services, facilities and devices, are at all times, the property of the department*]

Responsibilities and obligations

[*Outlines both departmental and employee responsibilities and obligations when using ICT services, facilities and devices*]

Training

[*Outlines how the department will address training of employees in the use of ICT services, facilities and devices. A sample acknowledgement form is attached*]

Monitoring

[*States the department’s processes and objectives for monitoring employee use of ICT services, facilities and devices*]

External email monitoring

[*States the department’s processes and objectives for monitoring external emails*]

Disciplinary procedures

[*Clearly identify disciplinary procedures to deal with unlawful or criminal use of ICT services, facilities and devices, indicate that employees have a right of appeal in relation to a department undertaking disciplinary action and outlines penalties for misuse*]

Example process – receipt of inappropriate emails

If an employee regularly receives unauthorised emails from a particular source, it is no defence to say that the emails were unsolicited if the employee does not take action to prevent this from continuing.

If an employee regularly received inappropriate emails from a particular source or sources, they should take action to prevent this continuing. Depending on the circumstances the employee should take the action specified in paragraphs 1 and 2 or 1 and 3:

1. Inform the employee’s supervisor of the receipt of inappropriate emails.
2. Inform the sender by email that the sender must not forward any further inappropriate email transmissions to the employee and provide the employee’s supervisor with a copy of that email.
3. Report to the departmental IT unit the receipt of inappropriate emails. The IT unit may block all further email transmissions from that sender.

Example of employee agreement on the use of the internet and email

I acknowledge that I have read and understood (department name) internet and email policy and will act in accordance with this policy and any other appropriate State and Commonwealth legislation.

In particular, I understand that:

* use of internet and email will be for authorised purposes only
* use of internet and email on government-owned ICT services, facilities and devices may be monitored by authorised personnel
* unauthorised use of internet and email may result in penalties including removal of the privilege of using internet and email, dismissal and/or criminal charges.

|  |  |
| --- | --- |
| Signed: |  |
| Name: |  |
| Position: |  |
| Date: |  |

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Key changes made** |
| 1.0.0 | July 2012 | Queensland Government Chief Information Office | Approved |
| 1.0.1 | October 2014 | Queensland Government Chief Information Office | Updated to new template for review |
| 1.0.2 | April 2015 |  |  |
| 1.0.3 | September 2015 | Queensland Government Chief Information Office | Links checked, minor updates. |
| 1.0.4 | September 2015 | Queensland Government Chief Information Office | Preparation for informal consultation. |
| 1.0.5-1.0.6 | September 2015 | Queensland Government Chief Information Office | Final amendments for formal consultation. |
| 1.1.0 | October 2015 | Queensland Government Chief Information Office | Formal consultation version |
| 1.1.1 | October 2015 | QGCIO | Incorporation of formal feedback and feedback from R. Mead. |
| 2.0.0 | December 2015 | QGCIO | Approved for publishing |
| 2.0.1 | March 2017 | QGCIO | Update links |
| 2.0.3 | November 2020 | QGEA team | References to Email monitoring and the Telecommunications (Interception and Access) guideline & FAQ’s highlighted for deletion as per email from Chantel Helmore on 18.11.20 |