

Department of Justice and Attorney General

Information Technology Services

# Use of ICT Services, Facilities and Devices Policy

## Document information

Security classification	UNCLASSIFIED		
Date of review of security classification	June 2017		
Authority	Executive Director, Information Technology Services		
Documentation status	Final	Consultation release	<input checked="" type="checkbox"/> Final version
Next review date	June 2019		
Document reference	eDOCS number: 3711798		

## Version history

Version	Notes	Author	Date of change
1.0	Approved by IMC as the Information Management Branch's Use of Information and Communication Technology (ICT) Devices Policy	-	March 2005
2.0	Changed to IMB Policy Template and minor editing amendments that do not change context of document	Terry McDonald	July 2005
3.0	Review, update and major change of policy – merging telecommunications, BlackBerry and ICT devices and facilities into one policy.	Marija Mamic	March 2007
4.0	Full redraft covering latest QGCIO IS38 update, currency for DJAG, comparison to other state government department published policies and increased definition and examples on misuse of information and Authorised/Unauthorised use.	Raamon Vaccaro	June 2016
5.0	Further update and review from consultation.	Brenda Lee	12 July 2016
6.0	Final version replaces all previous versions of the Information Management Branch's Use of Information and Communication Technology (ICT) Devices Policy, and Information & Communication Technology Branch's Internet and Email Usage Standards.	Brenda Lee	23 January 2017

## Policy owner/enquiries

Direct all enquiries and assistance regarding use of ICT services, facilities and devices, including any suggested updates and changes to this policy to the Justice IT Service Desk on 3239 0001 or by email [justiceitservicedesk@justice.qld.gov.au](mailto:justiceitservicedesk@justice.qld.gov.au).

This policy is owned by the Executive Director, ITS, who is responsible for the development and ongoing review of the policy.

## Policy approval and review

This policy was endorsed by the departmental Information and Technology Innovation Committee (ITIC) on 8 June 2017.

This policy was approved by David Mackie, Director-General, Department of Justice and Attorney-General on 13 July 2017.

The Executive Director, Information Technology Services, Department of Justice and Attorney-General is responsible for the development and ongoing review of this policy.

This policy will be reviewed at least every two years. The next scheduled review is June 2019.

---

## Security classification

This document has a security classification of UNCLASSIFIED.

## License

Use of ICT services, facilities and devices policy © The State of Queensland (Department of Justice and Attorney-General) 2017.



<http://creativecommons.org/licenses/by/4.0/deed.en>

This work is licensed under a Creative Commons Attribution 4.0 International Licence. You are free to copy, communicate and adapt this work, as long as you attribute by citing 'Use of ICT services, facilities and devices policy, State of Queensland (Department of Justice and Attorney-General) 2017'.

---

## 1. Purpose

This policy addresses employee use and the monitoring of ICT services, facilities and devices with the Department of Justice and Attorney-General (DJAG). It will:

- set clear expectations for employees on what the department considers appropriate and authorised use of ICT services, facilities and devices, and
- ensure ICT services, facilities and devices are used by employees in a manner that is efficient, effective, minimises risks and can survive public scrutiny and/or disclosure<sup>1</sup>.

This policy supports the Queensland Government Chief Information Office's Use of ICT services, facilities and devices policy - IS38 and Public Service Commission's (PSC) Use of internet and email policy.

## 2. Applicability

This policy applies to all ICT services, facilities and devices (owned, leased or licensed), provided to employees to carry out their work, regardless of their location (online, in Australia or overseas).

For the purposes of this policy, employee refers to all DJAG staff, including temporary staff, contractors and consultants and any other person who provides a service on a paid or voluntary basis to DJAG.

## 3. Policy statement

The department provides employees with ICT services, facilities and devices on the basis they are used for activities defined in accordance with authorised use in section 5 this policy and legislative requirements, including the:

- Code of Conduct for the Queensland Public Service (Code of Conduct)
- *Public Sector Ethics Act 1994 (Qld)*
- *Public Service Act 2008 (Qld)*.

All employees are accountable for their actions while using departmental ICT services, facilities and devices, and must abide by the roles and responsibilities contained in section 9 of this policy.

Any use of ICT services by employees must:

- be able to withstand internal and public scrutiny and/or disclosure, and
- respect the dignity, rights and views of others.

Work documents, data, messages, email, correspondence and information created, received and/or stored on departmental devices or through other ICT facilities or services may constitute public records under the Public Records Act 2002 (Qld) and/or be subject to disclosure under the Right to Information Act 2009 (Qld), the Information Privacy Act 2009 (Qld) or subpoena.

The department has adopted a zero tolerance approach to the misuse / inappropriate use of its ICT services, facilities and devices.

The department will periodically review, assess and address any risks associated with the use of ICT services, facilities and devices and take appropriate action as needed.

The department will educate and inform employees on the use of ICT services, facilities and devices including their responsibilities<sup>2</sup> as set out in this policy.

---

<sup>1</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Policy benefits

<sup>2</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Requirement 2 and PSC's Use of internet and email policy, Principle 7.6

---

## 4. Provision and ownership

The department provides and/or allows devices be used to access the department's systems, software and other facilities and services.

### ***Departmental ICT devices***

ICT devices wholly purchased by the department are public resources and must be properly maintained, managed and protected against theft and damage. When managing ICT devices Information Technology Services Branch (ITS) under authorisation processes may remotely remove any departmentally provisioned service and associated data through these devices. This remote access may inadvertently remove an employee's limited personal data/information.

### ***Employee's personal ICT devices<sup>3</sup>***

An employee owned ICT device can access departmental email, OneDrive, calendar services through Office 365 and other Office 365 applications by using an ITS approved remote access solution. Other departmental ICT applications and services are not sanctioned for use on personal devices.

When accessing departmental information from a personal device, employees should ensure that they:

- understand they are responsible for any service billing or other financial charges associated with the device
- understand that the department will not assist in any issues relating to the device
- do not compromise the department's information security
- abide by authorised use requirements within this policy when using departmental ICT facilities and services and handling departmental information
- ensure only PUBLIC, UNCLASSIFIED and X-IN-CONFIDENCE information is created or used within the device
- understand that in the event of security breaches ITS may remotely wipe a departmentally approved system or program that has been implemented under a departmental licence or agreement, and in doing so the department may inadvertently remove their personal information.

Employees must remove departmental information from their personal device and cease accessing the department's services on the device:

- when it is no longer required for departmental work purposes
- upon leaving the employment of the department
- before any exchange of the equipment such as under warranty or for repair, or
- before disposal of the device.

While the department applies a range of security controls, it makes no warranties that access to the department's ICT services and facilities will be continuous, fault-free or secure. The department does not accept responsibility for any loss of personal data, delays, non-deliveries, service interruptions, technical difficulties or malicious activity arising, whether directly or indirectly, out of an employee's use of the department's ICT services and facilities on their own device.

## 5. Authorised use<sup>4</sup>

Using the department's ICT services, facilities and devices is authorised for the purposes of:

- a) conducting official business in pursuit of departmental objectives which means:

---

<sup>3</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Implementation guideline section 4.1

<sup>4</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Requirement 1, PSC's Use of internet and email policy and Principles Statement, Principles 7.2 and 7.3

- 
- i. accessing and/or using ICT services, facilities and devices and information specifically for work related purposes
  - ii. communicating with colleagues, external stakeholders or partners, on work related matters
  - b) supporting professional development, as approved by the employee's manager or supervisor, such as:
    - i. professional development relating to study or research in accordance with the department's Study and Research Assistance Scheme (SARAS) Policy
    - ii. approved forum, conference or seminar participation
    - iii. engaging with a professional or industrial organisation for membership, registration, training/education, performance, conduct or safety
  - c) undertaking work related to the Armed Forces (Reserve)
  - d) limited personal use.

When using departmental ICT services, facilities and devices, employees are also subject to the following conditions and must:

- prior to the access/use of any ICT services, facilities and devices read and acknowledge any terms and conditions provided
- follow any conditions of use
- not attempt to disable, prevent or circumvent any existing or future security measures
- not share their logon (user ID) and password information, and will be held personally responsible for any activity that has taken place by not managing their logon
- take all necessary precautions to prevent unauthorised use or theft including not leaving devices in an unlocked or unattended state
- comply with the PSC's Use of internet and email policy
- manage records in accordance with the department's Recordkeeping policy
- protect personal information in accordance with the Information Privacy Act 2009 (Qld)
- determine the information security classification of the information and protect it according to the applicable controls
- protect intellectual property including copyright
- respect the dignity, rights and views of others when communicating
- only use software or online services which has been authorised or purchased through ITS
- abide by software licenses, copyright including Creative Commons licences (AusGOAL) and any intellectual property requirements they use
- seek prior approval from their manager or supervisor before taking a departmental ICT device overseas and/or enabling international roaming.

See Attachment 1: Definitions for examples of authorised use.

### ***Limited personal use***

Limited personal use of ICT services, facilities and devices by employees means that it:

- a) incurs minimal additional expense, does not interfere with and does not affect the business activities of the department
- b) is brief and infrequent
- c) is not for or in connection with private business
- d) is able to withstand scrutiny of colleagues, the community and media
- e) does not unnecessarily impact on an employee's ability to undertake their duties
- f) is consistent with this policy and the Public Service Act 2008 and/or the Code of Conduct and does not violate any other departmental policy and state or Commonwealth policy, legislation or regulation regarding the use of ICT services, facilities and devices.

---

The department provides a personal drive (OneDrive or equivalent) for the storage of personal, ephemeral and reference information. It is the employees responsibility to ensure that any personal data/information is backed up and that these work related storage areas are not used as the primary location to store personal data.

Information and usage associated with limited personal use is also subject to the same access, retrieval, review and monitoring practices as employment related use and is subject to the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld).

The department does not accept liability for any loss or damage suffered as a result of an employee using departmental ICT services, facilities and devices for personal use.

Personal use of the department's ICT services, facilities and devices can be revoked at any time.

See Attachment 1: Definitions for examples of limited personal use.

Where employees have any doubt as to what is authorised use or limited personal use, must discuss this with their manager or supervisor.

## 6. Unauthorised use<sup>5</sup>

Access or use of any ICT services, facility or device that does not meet the conditions of authorised use will constitute unauthorised use, which is a manner that is inappropriate or unlawful by:

- a) failing to behave in a manner which supports the Public Service Act 2008 (Qld), the Code of Conduct, the Use of internet and email policy, this policy and other departmental policies and associated legislation (see **Attachment 2: References**)
- b) misusing information from departmental systems, including:
  - i. accessing departmental business information and systems without an authorised business purpose (e.g. emailing departmental documents to a personal email account for unauthorised purpose, selling information for personal profit, searching classified information to share with a friend, acquaintance or family member)
  - ii. searching records, including client records, on a departmental database without an authorised business purpose (for clarity this means that staff members are not permitted to browse client files for their own interest unless the staff member has a specific work related requirement to view those records. Additionally, it is not appropriate in any circumstance for staff members to view records of client/s that are known to them on a personal basis)
  - iii. distributing information from departmental business systems to the public or media
  - iv. handling classified information inappropriately
  - v. extracting, disclosing modifying, adding or deleting business information when not for a departmental purpose.

The PSC's Use of internet and email policy provides the consequences should an employee inappropriately uses the internet or email.

See Attachment 1: Definitions for examples of unauthorised use.

Where employees have any doubt as to what is unauthorised use, employees must discuss this with their manager or supervisor.

## 7. Accessing, monitoring and restrictions

The department logs and monitors departmental services on a daily basis using ICT networks, operating systems, applications, web servers, mail servers, gateways, log transactions and communications. Scanning occurs by virus protection software on any ICT device (personal or not) that is connected to the department's network such as a USB key.

---

<sup>5</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1



---

Monitoring may also occur at the manager or supervisor level for licenses, internet and printer usage, and access to systems to evaluate optimisation and cost efficiencies.

Incoming and outgoing email (including emails of a personal nature), and their attachments, are automatically scanned for the detection of viruses, suspect or malicious code, SPAM, executable programs, unacceptable size and unacceptable content. Emails that represent a clearly defined security or maintenance threat to the department's ICT network are automatically quarantined with a simultaneous notification message sent to the intended recipient. Suspect emails are kept for 30 days and thereafter automatically deleted.

To access ICT services or facilities from a non-corporate ICT device additional security may need to be established. This may include the use of an employee's personal mobile number in order to provide a security access code.

All actions regarding the use of ICT services, facilities and devices (including those of a personal nature) are legally a public record of government business. All use may be monitored, audited, recorded and reviewed for compliance with departmental policies, standards, legislation and Code of Conduct. Relevant information is disclosed with authorisation as deemed appropriate in the circumstances.

## **8. Non-compliance with this policy**

The department will manage all alleged breaches of this policy in accordance with Public Service Act 2008 (Qld) and the Code of Conduct. Employees breaching this policy may be subject to disciplinary action (including termination of employment) subject to the principles of natural justice.<sup>6</sup> A pattern of behaviour (e.g. repeated use) will be a factor for consideration in determining the penalty.

## **9. Roles and responsibilities**

### ***Employees***

All employees (see Attachment 1: Definitions) are responsible for:

- reporting lost, stolen or damaged ICT devices
- only using ICT services, facilities and devices for activities as defined in authorised use
- reporting instances of unauthorised use
- keeping the credentials of ICT systems secure (including user ID and passwords)
- returning departmental software and devices upon ceasing employment with the department
- protecting software or devices against theft and damage
- managing departmental information in accordance with the Information security policy and the Recordkeeping policy
- seeking clarification on this policy if they do not understand what is required of them.

Where an employee has any doubts about what is required of them, they must discuss with their manager or supervisor in the first instance. If further clarification is required, contact the Justice IT Service Desk.

### ***Managers or supervisors***

Managers or supervisors (see Attachment 1: Definitions), or their delegate, are responsible for:

- ensuring ongoing staff educating/awareness of this policy, including during induction
- notify the Justice IT Service Desk of employees ceasing employment or beginning long term leave /secondment from the department

---

<sup>6</sup> PSC's Use of internet and email policy, Principle 7.5



- 
- regularly reviewing employee access to ICT services, facilities and devices so that it is commensurate with the role being performed
  - ensuring employees receive sufficient education to use the department's ICT services, facilities and devices
  - ensuring all ICT purchases are made through ITS or with their approval in accordance with the Financial Management Practice Manual.

### ***Chief Information Officer and Information Technology Services, Corporate Services***

Information Technology Services (ITS), Corporate Services is responsible for:

- developing, maintaining and communicating this policy
- endorsing ICT purchases for the department as per Financial Management Practice Manual (Section 11.1.13)
- keeping scanning and monitoring software to ensure legislative and departmental policy requirements are met, with guidance and/or direction from the Executive Director, Human Resources, Director, Legal Advice and Advocacy, the Assistant Director-General Corporate Services, Ethical Standards Unit and/or Internal Audit, as required.

The Chief Information Officer is responsible for authorising:

- the monitoring of ICT services, facilities and devices
- access, retrieval and review of information and records from or related to ICT services, facilities and devices
- any investigation or inquiry being carried out by Ethical Standards Unit, Internal Audit or a manager.

### ***Director-General***

The Director-General or delegate is responsible for determining whether a breach of this policy has occurred and undertaking the appropriate course of action e.g. disciplinary action.

## **10. Reporting requirements**

Internal Audit may conduct audit reviews of ICT information systems (including system logs) to assess compliance of procedures, practices, behaviours, legal and administrative requirements. Details of employees disciplined for breaches of this policy and/or PSC's Use of internet and email policy subject to mandatory reporting requirements, may be referred to relevant law enforcement and/or oversight body (such as the Crime and Corruption Commission).

## Attachment 1: Definitions

For the purpose of this policy, the following definitions shall apply:

Term	Explanation
Authorised use <sup>7</sup>	<p>Authorised use of departmental ICT services, facilities and devices is restricted to the following activities:</p> <ul style="list-style-type: none"> <li>a) official business</li> <li>b) professional development</li> <li>c) armed forces related work, and</li> <li>d) limited personal use.</li> </ul> <p>For a more detailed explanation see section 5.</p> <p><b>Examples of <i>Authorised use</i> include but not limited to:</b></p> <ul style="list-style-type: none"> <li>• printing documents relating to a departmental training course</li> <li>• using the internet to perform departmental related case/project research</li> <li>• using email to communicate new departmental directives or policies</li> <li>• informing employees of new departmental initiatives and/or staff movements</li> <li>• placing a telephone call to other government agencies for the purpose of acquiring or sharing information.</li> </ul>
Blog	A web log usually set up as a personal journal that is publicly accessible.
Code of Conduct for the Queensland Public Service (Code of Conduct)	<u>Code of Conduct for the Queensland Public Service</u> sets out standards of behaviour for all Queensland public service agency employees, contractors, subcontractors (including employees of contractors and subcontractors), students and volunteers who work in any capacity for a Queensland public service agency.
Department	Department of Justice and Attorney-General
Digitisation	The creation of digital images from paper documents by such means as scanning or digital photography. <sup>8</sup>
DJAG	Department of Justice and Attorney-General
Employee	For the purposes of this policy, employee refers to all departmental staff, including temporary staff, contractors and consultants and any other person who provides a service on a paid or voluntary basis to the department. It excludes Judicial Officers and Judicial Associates, who are not public servants, are exempt from the requirement to abide by this policy.
Ephemeral information	Ephemeral documents are items of short-term temporary information value.
ICT	Information and communication technology
ICT devices	<p>Electronic equipment designed for a particular communication and/or function, including but not limited to:</p> <ul style="list-style-type: none"> <li>• computers (e.g. desktop computers, mobile devices, laptops, servers, consoles and handheld devices)</li> <li>• phones (including fixed lines, mobiles, smart phones and satellite telephones) and accessories to phones (including battery chargers, cables)</li> <li>• digital or analogue recorders and removable media (e.g. USBs, DVDs, video, portable hard drives)</li> <li>• radios or other high frequency communication devices</li> <li>• televisions, computer monitors and videoconferencing equipment</li> </ul>

<sup>7</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1 and Authorised and unauthorised use of ICT services, facilities and devices guideline.

<sup>8</sup> Queensland State Archives - Digitisation Disposal Policy, Policy for Queensland Public Authorities, August 2014

Term	Explanation
	<ul style="list-style-type: none"> <li>digital or analogue players/recorders (including DVD and video), cameras</li> <li>monitors and sensors</li> <li>printing, photocopying, facsimile, scanning machines and multi-function devices.</li> </ul>
ICT facilities	A telecommunication service designed for a particular communication and/or function, which includes but is not limited to IT networks and servers, IT systems, wireless networks, internet, extranet, email, instant messaging, webmail, fee-based web services and social media.
ICT services	Telecommunications or transmission services that carry voice and/or data and includes applications, hosting, storage, online services delivered over the web and cloud based services etc. The services includes software generally e.g. core business application, Microsoft suite of products such as the Office 365 service, and operating software on computers or servers.
ICT services, facilities and devices	See ICT services, ICT facilities and ICT devices within this definition attachment.
Information security classification	Information is classified according to the nature of the information and the possible damage it may cause for example, PUBLIC, UNCLASSIFIED or IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED. QGCIO's Information standard - IS18 mandates that all agency information assets are assigned appropriate classification which then determines the appropriate controls to handle those information assets <sup>9</sup> .
Intranet	The internal website usually accessed by a web-browser that is accessible by the department only, as it is restricted by a firewall.
IS	Queensland Government Chief Information Office's Information Standard.
ITS	Information Technology Services, part of the Corporate Services Division within the department.
Limited personal use	<p>Personal use of departmental ICT services, facilities and devices by employees means be brief, infrequent and at minimal cost to the department. For a more detailed explanation see Section 5.</p> <p><b>Examples of authorised limited personal use include but not limited to:</b></p> <ul style="list-style-type: none"> <li>using the internet to access a news website</li> <li>using a printer or photocopier to print out a few pages of personal information on limited occasions</li> <li>making or receiving brief local telephone calls, or sending mobile phone SMS messages, to a partner/friend in relation to work, family or other personal commitments</li> <li>using a fax or email to change personal banking details</li> <li>making financial transactions, including bill paying, home banking and purchasing non-work related goods and services which do not relate to a personal private business</li> <li>for those employees working offsite from departmental premises and away from home, using their personal email on a departmental device in order to manage personal affairs</li> <li>completing a job application</li> <li>printing and distributing information relating to professional training/seminar events</li> <li>conducting searches over the internet on appropriate and ethical topics that will not cause embarrassment or harm to the department</li> <li>reading personal internet based email is open to scrutiny and must not be inappropriate, unlawful or criminal and does not relate to a private business enterprise.</li> </ul>

<sup>9</sup> Queensland Government's Information Security Classification Framework.

Term	Explanation
	<p><b>Examples of unauthorised limited personal use include:</b></p> <ul style="list-style-type: none"> <li>• using a departmental telephone to call overseas telephone numbers for personal reasons where it is not an emergency situation</li> <li>• making personal phone calls or electronic communications of long duration</li> <li>• sending emails of a personal nature via a group distribution list without appropriate approval</li> <li>• using the departmental telephones, meeting room or videoconferencing facilities to conduct personal conference calls</li> <li>• using departmental photocopiers and/or printers to photocopy/print out a large amount of personal information such as flyers for a school fete</li> <li>• using governmental ICT equipment to express political views, whether utilising a government email account or a personal email account (e.g. via Gmail)</li> <li>• using your government email account to contribute to non-work-related online feedback forums, voting online or blog sites, or to submit personal comments online in response to current issues.</li> </ul>
Manager or supervisor	A role within the department that has responsibility, either directly or indirectly, of an employee.
Metadata	Data that describes other data. For example, recordkeeping metadata is information describing the context, content and structure of records and their management. Metadata allows for information management, such as improving search ability.
Monitoring	The process of checking, observing, tracking, recording and/or evaluating employees use of the department's ICT services, facilities and devices.
Non-corporate ICT device	Any ICT device not purchased or managed by the department to enable an employee to perform their work duties.
Online service	Use of the internet for information service delivery and/or collaboration with other government agencies and organisations external to the department.
Phishing	The act of sending an email to a user falsely claiming to be an established legitimate enterprise, in an attempt to induce the user into surrendering private information for an unlawful activity such as identity theft.
Policy	This Use of ICT services, facilities and devices policy document.
Public Safety Network (PSN)	A secure Queensland Government data network infrastructure that includes DJAG, Queensland Corrective Services, Queensland Police, Rural Fire, Queensland Ambulance and Queensland Fire.
Public service employee	A person employed under the <i>Public Service Act 2008 (Qld)</i> in agencies, departments or public service offices.
QGCIO	Queensland Government Chief Information Office.
Record	Records are recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the public authority's business or affairs. In the context of business systems, a record could be an entire business system, a row in a table or an extract of data in the form of a report <sup>10</sup> .
RDS	Remote desktop service.
Scanning and monitoring software	Software that monitors and tracks elements within or that pass through a computer network.
Spam	Unsolicited 'junk' email sent to large numbers of people, often from automated systems, to promote products or services.

<sup>10</sup> Queensland State Archives - Website [glossary](#)

Term	Explanation
Spyware	Any software that covertly gathers user information through the user's internet connection without his or her knowledge. Spyware is often used for advertising purposes and a spyware application is typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses, passwords and credit card numbers.
Trojan horse	A destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive.
Unauthorised use <sup>11</sup>	<p>Access or use of any ICT service, facility or device that does not meet the conditions of authorised use will constitute unauthorised use, which is a manner that is inappropriate or unlawful. Examples of unauthorised use include but limited to:</p> <ul style="list-style-type: none"> <li>a) downloading, storing or distributing pornography using departmental ICT services, facilities and devices</li> <li>b) taking inappropriate and/or pornographic pictures with a mobile phone camera or any other form of camera or portable device</li> <li>c) forwarding inappropriate jokes and graphics, particularly any material of a sexually explicit, racist, defamatory, indecent, obscure, profane or offensive nature</li> <li>d) maintaining or supporting a personal private business (including your own business or a family/friend's business), including fee-based or subscription services or stock trading</li> <li>e) creating or maintaining personal websites</li> <li>f) knowingly accessing or downloading website material that is defamatory, harassing or discriminatory or sending messages that are defamatory, harassing or discriminatory</li> <li>g) online gambling, stock trading or accessing dating services online</li> <li>h) downloading image/sound/movie files and records, such as photos, .mp3, .wav and .avi files or similar files in other formats, unless for official business purposes</li> <li>i) sending and/or downloading material such as chain letters or letters relating to pyramid schemes or in any way participating in such activities</li> <li>j) disrupting the department's ICT services, facilities and devices such as spamming or other forms of mass mailing, storing and/or transmitting large files or any other unnecessary activity that may place a burden on departmental resources</li> <li>k) knowingly downloading, sending and/or broadcasting material from the internet or email containing viruses, worms, time bombs, cancel bots, Trojan horses, spyware or any other contaminating or destructive features</li> <li>l) knowingly accessing internet sites and activities which a reasonable person would find offensive in the workplace or contain unlawful practices (e.g. bomb making instructions), except where related to an approved genuine departmental business requirement</li> <li>m) installing software on departmental ICT devices without firstly obtaining the approval from the manager or supervisor</li> </ul>

<sup>11</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1 and Authorised and unauthorised use of ICT services, facilities and devices guideline.

Term	Explanation
	<p>n) installing departmentally provisioned software on ICT devices personally owned by the employee, or installing instances of software where licensing isn't departmentally provisioned</p> <p>o) accessing, playing and/or distributing computer games or unlicensed software</p> <p>p) accessing internet streaming services, such as radio and television, video streams, sports broadcasts, simulcasts on any departmental owned ICT services, facilities and devices, except where related to an approved departmental business or education requirement</p> <p>q) accessing ICT services such as online chat and info call services (e.g. 1900 telephone numbers), unless for work purposes</p> <p>r) posting messages representing the department on the internet and/or any other public computer system without first obtaining the approval of a manager or supervisor</p> <p>s) representing personal opinions on the internet/email as those of the department, or otherwise failing to comply with departmental practices concerning public statements about the government's position</p> <p>t) transmitting proprietary information or confidential information related to clients, suppliers, vendors or trading partners (e.g. via email or other internet services)</p> <p>u) failing to comply with confidentiality agreements with third parties that may explicitly prohibit communication over public computer systems</p> <p>v) failing to keep secure the department's ICT system and software access 'logins' (user name) and passwords issued to employees, including the transmission of this information over the internet and/or via email accounts</p> <p>w) engaging in any form of phishing or obscuring the origins of any message or download material under an assumed internet address or otherwise disguise a user's identity</p> <p>x) altering the content of an email received without the sender's approval or without clearly indicating that you have altered the content</p> <p>y) infringing intellectual property rights of others (e.g. copying or downloading video or software where copyright does not permit) or unlawfully circumventing technological protection measures designed to deter copyright infringement</p> <p>z) deliberately misusing and/or not taking due care of departmental ICT devices</p> <p>aa) failing to adhere to safety requirements and restrictions on usage of devices (e.g. failing to adhere to mobile phone usage restrictions in designated hospital areas, failing to take care and/or using hands-free communication equipment when using a mobile phone whilst a vehicle is moving)</p> <p>bb) stealing departmental ICT services, facilities and devices and/or information</p> <p>cc) allowing unauthorised persons, whether external (e.g. friends or relatives) or internal to the department, to use the department's ICT services, facilities and devices</p> <p>dd) using ICT services, facilities and devices and/or departmental information in a way which waives or has the potential to waive the department's legal professional privilege in the contents of legal advice.</p> <p>For a more detailed explanation see Section 6.</p>

---

Term	Explanation
Virus	A computer program or piece of code that embeds into your computer files without your knowledge and runs against your wishes. Most viruses can also replicate themselves and spread to other computers. All computer viruses are man-made usually for malicious intent.
Worm	A computer program capable of reproducing itself that can spread from one computer to the next over a network. Worms take advantage of automatic file sending and receiving features found on many computers.



---

## Attachment 2: References

The requirements set out in this document are based on, and are consistent with, relevant government legislation, regulations, directives, information standards and/or policies at the time of publication.

### Departmental policies and procedures

Recordkeeping Policy

Information security policy

Information Security Plan

Financial Management Practice Manual

IT Equipment Collection & Disposal Form

### Queensland Government policies

Code of Conduct for the Queensland Public Service

Queensland Government Chief Information Office's Use of ICT services, facilities and devices policy – IS38

Public Service Commission's Use of Internet and email policy

Queensland Government Chief Information Office's Information Security – IS18 Information Standard

Queensland Government information security classification framework

Crime and Corruption Commission's Confidential information: unauthorised access, disclosure and the risks of corruption in the Queensland public sector

### Legislation and regulations

Crime and Corruption Act 2001 (Qld)

Information Privacy Act 2009 (Qld)

Public Sector Ethics Act 1994 (Qld)

Public Service Act 2008 (Qld)

Right to Information Act 2009 (Qld)

Public Records Act 2002 (Qld)

Department of Justice and Attorney General

Information Technology Services

# Use of ICT Services, Facilities and Devices Policy

## Document information

Security classification	UNCLASSIFIED		
Date of review of security classification	June 2017		
Authority	Executive Director, Information Technology Services		
Documentation status	Final	Consultation release	<input checked="" type="checkbox"/> Final version
Next review date	June 2019		
Document reference	eDOCS number: 3711798		

## Version history

Version	Notes	Author	Date of change
1.0	Approved by IMC as the Information Management Branch's Use of Information and Communication Technology (ICT) Devices Policy	-	March 2005
2.0	Changed to IMB Policy Template and minor editing amendments that do not change context of document	Terry McDonald	July 2005
3.0	Review, update and major change of policy – merging telecommunications, BlackBerry and ICT devices and facilities into one policy.	Marija Mamic	March 2007
4.0	Full redraft covering latest QGCIO IS38 update, currency for DJAG, comparison to other state government department published policies and increased definition and examples on misuse of information and Authorised/Unauthorised use.	Raamon Vaccaro	June 2016
5.0	Further update and review from consultation.	Brenda Lee	12 July 2016
6.0	Final version replaces all previous versions of the Information Management Branch's Use of Information and Communication Technology (ICT) Devices Policy, and Information & Communication Technology Branch's Internet and Email Usage Standards.	Brenda Lee	23 January 2017
7.0	Amendment to include DG directive to reflect usage of private email accounts should not to be used for government purposes, as documents may constitute records under public records act	Peter Waye	28 September 2017

## Policy owner/enquiries

Direct all enquiries and assistance regarding use of ICT services, facilities and devices, including any suggested updates and changes to this policy to the Justice IT Service Desk on 3239 0001 or by email [justiceitservicedesk@justice.qld.gov.au](mailto:justiceitservicedesk@justice.qld.gov.au).

This policy is owned by the Executive Director, ITS, who is responsible for the development and ongoing review of the policy.

## Policy approval and review

This policy was endorsed by the departmental Information and Technology Innovation Committee (ITIC) on 8 June 2017.

This policy was approved by David Mackie, Director-General, Department of Justice and Attorney-General on 13 July 2017.

---

The Executive Director, Information Technology Services, Department of Justice and Attorney-General is responsible for the development and ongoing review of this policy.

This policy will be reviewed at least every two years. The next scheduled review is June 2019.

### **Security classification**

This document has a security classification of UNCLASSIFIED.

### **License**

Use of ICT services, facilities and devices policy © The State of Queensland (Department of Justice and Attorney-General) 2017.



<http://creativecommons.org/licenses/by/4.0/deed.en>

This work is licensed under a Creative Commons Attribution 4.0 International Licence. You are free to copy, communicate and adapt this work, as long as you attribute by citing 'Use of ICT services, facilities and devices policy, State of Queensland (Department of Justice and Attorney-General) 2017'.

---

## 1. Purpose

This policy addresses employee use and the monitoring of ICT services, facilities and devices with the Department of Justice and Attorney-General (DJAG). It will:

- set clear expectations for employees on what the department considers appropriate and authorised use of ICT services, facilities and devices, and
- ensure ICT services, facilities and devices are used by employees in a manner that is efficient, effective, minimises risks and can survive public scrutiny and/or disclosure<sup>1</sup>.

This policy supports the Queensland Government Chief Information Office's Use of ICT services, facilities and devices policy - IS38 and Public Service Commission's (PSC) Use of internet and email policy.

## 2. Applicability

This policy applies to all ICT services, facilities and devices (owned, leased or licensed), provided to employees to carry out their work, regardless of their location (online, in Australia or overseas).

For the purposes of this policy, employee refers to all DJAG staff, including temporary staff, contractors and consultants and any other person who provides a service on a paid or voluntary basis to DJAG.

## 3. Policy statement

The department provides employees with ICT services, facilities and devices on the basis they are used for activities defined in accordance with authorised use in section 5 this policy and legislative requirements, including the:

- Code of Conduct for the Queensland Public Service (Code of Conduct)
- *Public Sector Ethics Act 1994 (Qld)*
- *Public Service Act 2008 (Qld)*.

All employees are accountable for their actions while using departmental ICT services, facilities and devices, and must abide by the roles and responsibilities contained in section 9 of this policy.

Any use of ICT services by employees must:

- be able to withstand internal and public scrutiny and/or disclosure, and
- respect the dignity, rights and views of others.

Work documents, data, messages, email, correspondence and information created, received and/or stored on departmental devices or through other ICT facilities or services may constitute public records under the Public Records Act 2002 (Qld) and/or be subject to disclosure under the Right to Information Act 2009 (Qld), the Information Privacy Act 2009 (Qld) or subpoena.

The department has adopted a zero tolerance approach to the misuse / inappropriate use of its ICT services, facilities and devices.

The department will periodically review, assess and address any risks associated with the use of ICT services, facilities and devices and take appropriate action as needed.

The department will educate and inform employees on the use of ICT services, facilities and devices including their responsibilities<sup>2</sup> as set out in this policy.

---

<sup>1</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Policy benefits

<sup>2</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Requirement 2 and PSC's Use of internet and email policy, Principle 7.6

---

## 4. Provision and ownership

The department provides and/or allows devices be used to access the department's systems, software and other facilities and services.

### ***Departmental ICT devices***

ICT devices wholly purchased by the department are public resources and must be properly maintained, managed and protected against theft and damage. When managing ICT devices Information Technology Services Branch (ITS) under authorisation processes may remotely remove any departmentally provisioned service and associated data through these devices. This remote access may inadvertently remove an employee's limited personal data/information.

### ***Employee's personal ICT devices<sup>3</sup>***

An employee owned ICT device can access departmental email, OneDrive, calendar services through Office 365 and other Office 365 applications by using an ITS approved remote access solution. Other departmental ICT applications and services are not sanctioned for use on personal devices.

When accessing departmental information from a personal device, employees should ensure that they:

- understand they are responsible for any service billing or other financial charges associated with the device
- understand that the department will not assist in any issues relating to the device
- do not compromise the department's information security
- abide by authorised use requirements within this policy when using departmental ICT facilities and services and handling departmental information
- ensure only PUBLIC, UNCLASSIFIED and X-IN-CONFIDENCE information is created or used within the device
- understand that in the event of security breaches ITS may remotely wipe a departmentally approved system or program that has been implemented under a departmental licence or agreement, and in doing so the department may inadvertently remove their personal information.

Employees must remove departmental information from their personal device and cease accessing the department's services on the device:

- when it is no longer required for departmental work purposes
- upon leaving the employment of the department
- before any exchange of the equipment such as under warranty or for repair, or
- before disposal of the device.

While the department applies a range of security controls, it makes no warranties that access to the department's ICT services and facilities will be continuous, fault-free or secure. The department does not accept responsibility for any loss of personal data, delays, non-deliveries, service interruptions, technical difficulties or malicious activity arising, whether directly or indirectly, out of an employee's use of the department's ICT services and facilities on their own device.

## 5. Authorised use<sup>4</sup>

Using the department's ICT services, facilities and devices is authorised for the purposes of:

- a) conducting official business in pursuit of departmental objectives which means:

---

<sup>3</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Implementation guideline section 4.1

<sup>4</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Requirement 1, PSC's Use of internet and email policy and Principles Statement, Principles 7.2 and 7.3

- 
- i. accessing and/or using ICT services, facilities and devices and information specifically for work related purposes
  - ii. communicating with colleagues, external stakeholders or partners, on work related matters
  - b) supporting professional development, as approved by the employee's manager or supervisor, such as:
    - i. professional development relating to study or research in accordance with the department's Study and Research Assistance Scheme (SARAS) Policy
    - ii. approved forum, conference or seminar participation
    - iii. engaging with a professional or industrial organisation for membership, registration, training/education, performance, conduct or safety
  - c) undertaking work related to the Armed Forces (Reserve)
  - d) limited personal use.

When using departmental ICT services, facilities and devices, employees are also subject to the following conditions and must:

- prior to the access/use of any ICT services, facilities and devices read and acknowledge any terms and conditions provided
- follow any conditions of use
- not attempt to disable, prevent or circumvent any existing or future security measures
- not share their logon (user ID) and password information, and will be held personally responsible for any activity that has taken place by not managing their logon
- take all necessary precautions to prevent unauthorised use or theft including not leaving devices in an unlocked or unattended state
- comply with the PSC's Use of internet and email policy
- manage records in accordance with the department's Recordkeeping policy
- protect personal information in accordance with the Information Privacy Act 2009 (Qld)
- determine the information security classification of the information and protect it according to the applicable controls
- protect intellectual property including copyright
- respect the dignity, rights and views of others when communicating
- only use software or online services which has been authorised or purchased through ITS
- abide by software licenses, copyright including Creative Commons licences (AusGOAL) and any intellectual property requirements they use
- seek prior approval from their manager or supervisor before taking a departmental ICT device overseas and/or enabling international roaming.

See Attachment 1: Definitions for examples of authorised use.

### ***Limited personal use***

Limited personal use of ICT services, facilities and devices by employees means that it:

- a) incurs minimal additional expense, does not interfere with and does not affect the business activities of the department
- b) is brief and infrequent
- c) is not for or in connection with private business
- d) is able to withstand scrutiny of colleagues, the community and media
- e) does not unnecessarily impact on an employee's ability to undertake their duties
- f) is consistent with this policy and the Public Service Act 2008 and/or the Code of Conduct and does not violate any other departmental policy and state or Commonwealth policy, legislation or regulation regarding the use of ICT services, facilities and devices.



---

The department provides a personal drive (OneDrive or equivalent) for the storage of personal, ephemeral and reference information. It is the employees responsibility to ensure that any personal data/information is backed up and that these work related storage areas are not used as the primary location to store personal data.

Information and usage associated with limited personal use is also subject to the same access, retrieval, review and monitoring practices as employment related use and is subject to the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld).

The department does not accept liability for any loss or damage suffered as a result of an employee using departmental ICT services, facilities and devices for personal use.

Personal use of the department's ICT services, facilities and devices can be revoked at any time.

See Attachment 1: Definitions for examples of limited personal use.

Where employees have any doubt as to what is authorised use or limited personal use, must discuss this with their manager or supervisor.

## 6. Unauthorised use<sup>5</sup>

Access or use of any ICT services, facility or device that does not meet the conditions of authorised use will constitute unauthorised use, which is a manner that is inappropriate or unlawful by:

- a) failing to behave in a manner which supports the Public Service Act 2008 (Qld), the Code of Conduct, the Use of internet and email policy, this policy and other departmental policies and associated legislation (see **Attachment 2: References**)

Private email accounts (or communication services such as text messages) should not be used for government-related business.

- b) misusing information from departmental systems, including:
- i. accessing departmental business information and systems without an authorised business purpose (e.g. emailing departmental documents to a personal email account for unauthorised purpose, selling information for personal profit, searching classified information to share with a friend, acquaintance or family member)
  - ii. searching records, including client records, on a departmental database without an authorised business purpose (for clarity this means that staff members are not permitted to browse client files for their own interest unless the staff member has a specific work related requirement to view those records. Additionally, it is not appropriate in any circumstance for staff members to view records of client/s that are known to them on a personal basis)
  - iii. distributing information from departmental business systems to the public or media
  - iv. handling classified information inappropriately
  - v. extracting, disclosing, modifying, adding or deleting business information when not for a departmental purpose.

The PSC's Use of internet and email policy provides the consequences should an employee inappropriately uses the internet or email.

See Attachment 1: Definitions for examples of unauthorised use.

Where employees have any doubt as to what is unauthorised use, employees must discuss this with their manager or supervisor.

---

<sup>5</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1

---

## 7. Accessing, monitoring and restrictions

The department logs and monitors departmental services on a daily basis using ICT networks, operating systems, applications, web servers, mail servers, gateways, log transactions and communications. Scanning occurs by virus protection software on any ICT device (personal or not) that is connected to the department's network such as a USB key. Monitoring may also occur at the manager or supervisor level for licenses, internet and printer usage, and access to systems to evaluate optimisation and cost efficiencies.

Incoming and outgoing email (including emails of a personal nature), and their attachments, are automatically scanned for the detection of viruses, suspect or malicious code, SPAM, executable programs, unacceptable size and unacceptable content. Emails that represent a clearly defined security or maintenance threat to the department's ICT network are automatically quarantined with a simultaneous notification message sent to the intended recipient. Suspect emails are kept for 30 days and thereafter automatically deleted.

To access ICT services or facilities from a non-corporate ICT device additional security may need to be established. This may include the use of an employee's personal mobile number in order to provide a security access code.

All actions regarding the use of ICT services, facilities and devices (including those of a personal nature) are legally a public record of government business. All use may be monitored, audited, recorded and reviewed for compliance with departmental policies, standards, legislation and Code of Conduct. Relevant information is disclosed with authorisation as deemed appropriate in the circumstances.

## 8. Non-compliance with this policy

The department will manage all alleged breaches of this policy in accordance with Public Service Act 2008 (Qld) and the Code of Conduct. Employees breaching this policy may be subject to disciplinary action (including termination of employment) subject to the principles of natural justice.<sup>6</sup> A pattern of behaviour (e.g. repeated use) will be a factor for consideration in determining the penalty.

## 9. Roles and responsibilities

### ***Employees***

All employees (see Attachment 1: Definitions) are responsible for:

- reporting lost, stolen or damaged ICT devices
- only using ICT services, facilities and devices for activities as defined in authorised use
- reporting instances of unauthorised use
- keeping the credentials of ICT systems secure (including user ID and passwords)
- returning departmental software and devices upon ceasing employment with the department
- protecting software or devices against theft and damage
- managing departmental information in accordance with the Information security policy and the Recordkeeping policy
- seeking clarification on this policy if they do not understand what is required of them.

Where an employee has any doubts about what is required of them, they must discuss with their manager or supervisor in the first instance. If further clarification is required, contact the Justice IT Service Desk.

---

<sup>6</sup> PSC's Use of internet and email policy, Principle 7.5

---

## ***Managers or supervisors***

Managers or supervisors (see Attachment 1: Definitions), or their delegate, are responsible for:

- ensuring ongoing staff educating/awareness of this policy, including during induction
- notify the Justice IT Service Desk of employees ceasing employment or beginning long term leave /secondment from the department
- regularly reviewing employee access to ICT services, facilities and devices so that it is commensurate with the role being performed
- ensuring employees receive sufficient education to use the department's ICT services, facilities and devices
- ensuring all ICT purchases are made through ITS or with their approval in accordance with the Financial Management Practice Manual.

## ***Chief Information Officer and Information Technology Services, Corporate Services***

Information Technology Services (ITS), Corporate Services is responsible for:

- developing, maintaining and communicating this policy
- endorsing ICT purchases for the department as per Financial Management Practice Manual (Section 11.1.13)
- keeping scanning and monitoring software to ensure legislative and departmental policy requirements are met, with guidance and/or direction from the Executive Director, Human Resources, Director, Legal Advice and Advocacy, the Assistant Director-General Corporate Services, Ethical Standards Unit and/or Internal Audit, as required.

The Chief Information Officer is responsible for authorising:

- the monitoring of ICT services, facilities and devices
- access, retrieval and review of information and records from or related to ICT services, facilities and devices
- any investigation or inquiry being carried out by Ethical Standards Unit, Internal Audit or a manager.

## ***Director-General***

The Director-General or delegate is responsible for determining whether a breach of this policy has occurred and undertaking the appropriate course of action e.g. disciplinary action.

## **10. Reporting requirements**

Internal Audit may conduct audit reviews of ICT information systems (including system logs) to assess compliance of procedures, practices, behaviours, legal and administrative requirements. Details of employees disciplined for breaches of this policy and/or PSC's Use of internet and email policy subject to mandatory reporting requirements, may be referred to relevant law enforcement and/or oversight body (such as the Crime and Corruption Commission).

## Attachment 1: Definitions

For the purpose of this policy, the following definitions shall apply:

Term	Explanation
Authorised use <sup>7</sup>	<p>Authorised use of departmental ICT services, facilities and devices is restricted to the following activities:</p> <ul style="list-style-type: none"> <li>a) official business</li> <li>b) professional development</li> <li>c) armed forces related work, and</li> <li>d) limited personal use.</li> </ul> <p>For a more detailed explanation see section 5.</p> <p><b>Examples of <i>Authorised use</i> include but not limited to:</b></p> <ul style="list-style-type: none"> <li>• printing documents relating to a departmental training course</li> <li>• using the internet to perform departmental related case/project research</li> <li>• using email to communicate new departmental directives or policies</li> <li>• informing employees of new departmental initiatives and/or staff movements</li> <li>• placing a telephone call to other government agencies for the purpose of acquiring or sharing information.</li> </ul>
Blog	A web log usually set up as a personal journal that is publicly accessible.
Code of Conduct for the Queensland Public Service (Code of Conduct)	<u>Code of Conduct for the Queensland Public Service</u> sets out standards of behaviour for all Queensland public service agency employees, contractors, subcontractors (including employees of contractors and subcontractors), students and volunteers who work in any capacity for a Queensland public service agency.
Department	Department of Justice and Attorney-General
Digitisation	The creation of digital images from paper documents by such means as scanning or digital photography. <sup>8</sup>
DJAG	Department of Justice and Attorney-General
Employee	For the purposes of this policy, employee refers to all departmental staff, including temporary staff, contractors and consultants and any other person who provides a service on a paid or voluntary basis to the department. It excludes Judicial Officers and Judicial Associates, who are not public servants, are exempt from the requirement to abide by this policy.
Ephemeral information	Ephemeral documents are items of short-term temporary information value.
ICT	Information and communication technology
ICT devices	<p>Electronic equipment designed for a particular communication and/or function, including but not limited to:</p> <ul style="list-style-type: none"> <li>• computers (e.g. desktop computers, mobile devices, laptops, servers, consoles and handheld devices)</li> <li>• phones (including fixed lines, mobiles, smart phones and satellite telephones) and accessories to phones (including battery chargers, cables)</li> <li>• digital or analogue recorders and removable media (e.g. USBs, DVDs, video, portable hard drives)</li> <li>• radios or other high frequency communication devices</li> <li>• televisions, computer monitors and videoconferencing equipment</li> </ul>

<sup>7</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1 and Authorised and unauthorised use of ICT services, facilities and devices guideline.

<sup>8</sup> Queensland State Archives - Digitisation Disposal Policy, Policy for Queensland Public Authorities, August 2014

Term	Explanation
	<ul style="list-style-type: none"> <li>digital or analogue players/recorders (including DVD and video), cameras</li> <li>monitors and sensors</li> <li>printing, photocopying, facsimile, scanning machines and multi-function devices.</li> </ul>
ICT facilities	A telecommunication service designed for a particular communication and/or function, which includes but is not limited to IT networks and servers, IT systems, wireless networks, internet, extranet, email, instant messaging, webmail, fee-based web services and social media.
ICT services	Telecommunications or transmission services that carry voice and/or data and includes applications, hosting, storage, online services delivered over the web and cloud based services etc. The services includes software generally e.g. core business application, Microsoft suite of products such as the Office 365 service, and operating software on computers or servers.
ICT services, facilities and devices	See ICT services, ICT facilities and ICT devices within this definition attachment.
Information security classification	Information is classified according to the nature of the information and the possible damage it may cause for example, PUBLIC, UNCLASSIFIED or IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED. QGCIO's Information standard - IS18 mandates that all agency information assets are assigned appropriate classification which then determines the appropriate controls to handle those information assets <sup>9</sup> .
Intranet	The internal website usually accessed by a web-browser that is accessible by the department only, as it is restricted by a firewall.
IS	Queensland Government Chief Information Office's Information Standard.
ITS	Information Technology Services, part of the Corporate Services Division within the department.
Limited personal use	<p>Personal use of departmental ICT services, facilities and devices by employees means be brief, infrequent and at minimal cost to the department. For a more detailed explanation see Section 5.</p> <p><b>Examples of authorised limited personal use include but not limited to:</b></p> <ul style="list-style-type: none"> <li>using the internet to access a news website</li> <li>using a printer or photocopier to print out a few pages of personal information on limited occasions</li> <li>making or receiving brief local telephone calls, or sending mobile phone SMS messages, to a partner/friend in relation to work, family or other personal commitments</li> <li>using a fax or email to change personal banking details</li> <li>making financial transactions, including bill paying, home banking and purchasing non-work related goods and services which do not relate to a personal private business</li> <li>for those employees working offsite from departmental premises and away from home, using their personal email on a departmental device in order to manage personal affairs</li> <li>completing a job application</li> <li>printing and distributing information relating to professional training/seminar events</li> <li>conducting searches over the internet on appropriate and ethical topics that will not cause embarrassment or harm to the department</li> <li>reading personal internet based email is open to scrutiny and must not be inappropriate, unlawful or criminal and does not relate to a private business enterprise.</li> </ul>

<sup>9</sup> Queensland Government's Information Security Classification Framework.

Term	Explanation
	<p><b>Examples of unauthorised limited personal use include:</b></p> <ul style="list-style-type: none"> <li>• using a departmental telephone to call overseas telephone numbers for personal reasons where it is not an emergency situation</li> <li>• making personal phone calls or electronic communications of long duration</li> <li>• sending emails of a personal nature via a group distribution list without appropriate approval</li> <li>• using the departmental telephones, meeting room or videoconferencing facilities to conduct personal conference calls</li> <li>• using departmental photocopiers and/or printers to photocopy/print out a large amount of personal information such as flyers for a school fete</li> <li>• using governmental ICT equipment to express political views, whether utilising a government email account or a personal email account (e.g. via Gmail)</li> <li>• using your government email account to contribute to non-work-related online feedback forums, voting online or blog sites, or to submit personal comments online in response to current issues.</li> </ul>
Manager or supervisor	A role within the department that has responsibility, either directly or indirectly, of an employee.
Metadata	Data that describes other data. For example, recordkeeping metadata is information describing the context, content and structure of records and their management. Metadata allows for information management, such as improving search ability.
Monitoring	The process of checking, observing, tracking, recording and/or evaluating employees use of the department's ICT services, facilities and devices.
Non-corporate ICT device	Any ICT device not purchased or managed by the department to enable an employee to perform their work duties.
Online service	Use of the internet for information service delivery and/or collaboration with other government agencies and organisations external to the department.
Phishing	The act of sending an email to a user falsely claiming to be an established legitimate enterprise, in an attempt to induce the user into surrendering private information for an unlawful activity such as identity theft.
Policy	This Use of ICT services, facilities and devices policy document.
Public Safety Network (PSN)	A secure Queensland Government data network infrastructure that includes DJAG, Queensland Corrective Services, Queensland Police, Rural Fire, Queensland Ambulance and Queensland Fire.
Public service employee	A person employed under the <i>Public Service Act 2008 (Qld)</i> in agencies, departments or public service offices.
QGCIO	Queensland Government Chief Information Office.
Record	Records are recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the public authority's business or affairs. In the context of business systems, a record could be an entire business system, a row in a table or an extract of data in the form of a report <sup>10</sup> .
RDS	Remote desktop service.
Scanning and monitoring software	Software that monitors and tracks elements within or that pass through a computer network.
Spam	Unsolicited 'junk' email sent to large numbers of people, often from automated systems, to promote products or services.

<sup>10</sup> Queensland State Archives - Website [glossary](#)



Term	Explanation
Spyware	Any software that covertly gathers user information through the user's internet connection without his or her knowledge. Spyware is often used for advertising purposes and a spyware application is typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses, passwords and credit card numbers.
Trojan horse	A destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive.
Unauthorised use <sup>11</sup>	<p>Access or use of any ICT service, facility or device that does not meet the conditions of authorised use will constitute unauthorised use, which is a manner that is inappropriate or unlawful. Examples of unauthorised use include but limited to:</p> <ul style="list-style-type: none"> <li>a) downloading, storing or distributing pornography using departmental ICT services, facilities and devices</li> <li>b) taking inappropriate and/or pornographic pictures with a mobile phone camera or any other form of camera or portable device</li> <li>c) forwarding inappropriate jokes and graphics, particularly any material of a sexually explicit, racist, defamatory, indecent, obscene, profane or offensive nature</li> <li>d) maintaining or supporting a personal private business (including your own business or a family/friend's business), including fee-based or subscription services or stock trading</li> <li>e) creating or maintaining personal websites</li> <li>f) knowingly accessing or downloading website material that is defamatory, harassing or discriminatory or sending messages that are defamatory, harassing or discriminatory</li> <li>g) online gambling, stock trading or accessing dating services online</li> <li>h) downloading image/sound/movie files and records, such as photos, .mp3, .wav and .avi files or similar files in other formats, unless for official business purposes</li> <li>i) sending and/or downloading material such as chain letters or letters relating to pyramid schemes or in any way participating in such activities</li> <li>j) disrupting the department's ICT services, facilities and devices such as spamming or other forms of mass mailing, storing and/or transmitting large files or any other unnecessary activity that may place a burden on departmental resources</li> <li>k) knowingly downloading, sending and/or broadcasting material from the internet or email containing viruses, worms, time bombs, cancel bots, Trojan horses, spyware or any other contaminating or destructive features</li> <li>l) knowingly accessing internet sites and activities which a reasonable person would find offensive in the workplace or contain unlawful practices (e.g. bomb making instructions), except where related to an approved genuine departmental business requirement</li> <li>m) installing software on departmental ICT devices without firstly obtaining the approval from the manager or supervisor</li> </ul>

<sup>11</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1 and Authorised and unauthorised use of ICT services, facilities and devices guideline.



Term	Explanation
	<p>n) installing departmentally provisioned software on ICT devices personally owned by the employee, or installing instances of software where licensing isn't departmentally provisioned</p> <p>o) accessing, playing and/or distributing computer games or unlicensed software</p> <p>p) accessing internet streaming services, such as radio and television, video streams, sports broadcasts, simulcasts on any departmental owned ICT services, facilities and devices, except where related to an approved departmental business or education requirement</p> <p>q) accessing ICT services such as online chat and info call services (e.g. 1900 telephone numbers), unless for work purposes</p> <p>r) posting messages representing the department on the internet and/or any other public computer system without first obtaining the approval of a manager or supervisor</p> <p>s) representing personal opinions on the internet/email as those of the department, or otherwise failing to comply with departmental practices concerning public statements about the government's position</p> <p>t) transmitting proprietary information or confidential information related to clients, suppliers, vendors or trading partners (e.g. via email or other internet services)</p> <p>u) failing to comply with confidentiality agreements with third parties that may explicitly prohibit communication over public computer systems</p> <p>v) failing to keep secure the department's ICT system and software access 'logins' (user name) and passwords issued to employees, including the transmission of this information over the internet and/or via email accounts</p> <p>w) engaging in any form of phishing or obscuring the origins of any message or download material under an assumed internet address or otherwise disguise a user's identity</p> <p>x) altering the content of an email received without the sender's approval or without clearly indicating that you have altered the content</p> <p>y) infringing intellectual property rights of others (e.g. copying or downloading video or software where copyright does not permit) or unlawfully circumventing technological protection measures designed to deter copyright infringement</p> <p>z) deliberately misusing and/or not taking due care of departmental ICT devices</p> <p>aa) failing to adhere to safety requirements and restrictions on usage of devices (e.g. failing to adhere to mobile phone usage restrictions in designated hospital areas, failing to take care and/or using hands-free communication equipment when using a mobile phone whilst a vehicle is moving)</p> <p>bb) stealing departmental ICT services, facilities and devices and/or information</p> <p>cc) allowing unauthorised persons, whether external (e.g. friends or relatives) or internal to the department, to use the department's ICT services, facilities and devices</p> <p>dd) using ICT services, facilities and devices and/or departmental information in a way which waives or has the potential to waive the department's legal professional privilege in the contents of legal advice</p> <p>ee) private email accounts (or communication services such as text messages) should not be used for <u>government-related business</u>.</p> <p>For a more detailed explanation, see Section 6.</p>

---

Term	Explanation
Virus	A computer program or piece of code that embeds into your computer files without your knowledge and runs against your wishes. Most viruses can also replicate themselves and spread to other computers. All computer viruses are man-made usually for malicious intent.
Worm	A computer program capable of reproducing itself that can spread from one computer to the next over a network. Worms take advantage of automatic file sending and receiving features found on many computers.

---

## Attachment 2: References

The requirements set out in this document are based on, and are consistent with, relevant government legislation, regulations, directives, information standards and/or policies at the time of publication.

### Departmental policies and procedures

Recordkeeping Policy

Information security policy

Information Security Plan

Financial Management Practice Manual

IT Equipment Collection & Disposal Form

### Queensland Government policies

Code of Conduct for the Queensland Public Service

Queensland Government Chief Information Office's Use of ICT services, facilities and devices policy – IS38

Public Service Commission's Use of Internet and email policy

Queensland Government Chief Information Office's Information Security – IS18 Information Standard

Queensland Government information security classification framework

Crime and Corruption Commission's Confidential information: unauthorised access, disclosure and the risks of corruption in the Queensland public sector

### Legislation and regulations

Crime and Corruption Act 2001 (Qld)

Information Privacy Act 2009 (Qld)

Public Sector Ethics Act 1994 (Qld)

Public Service Act 2008 (Qld)

Right to Information Act 2009 (Qld)

Public Records Act 2002 (Qld)

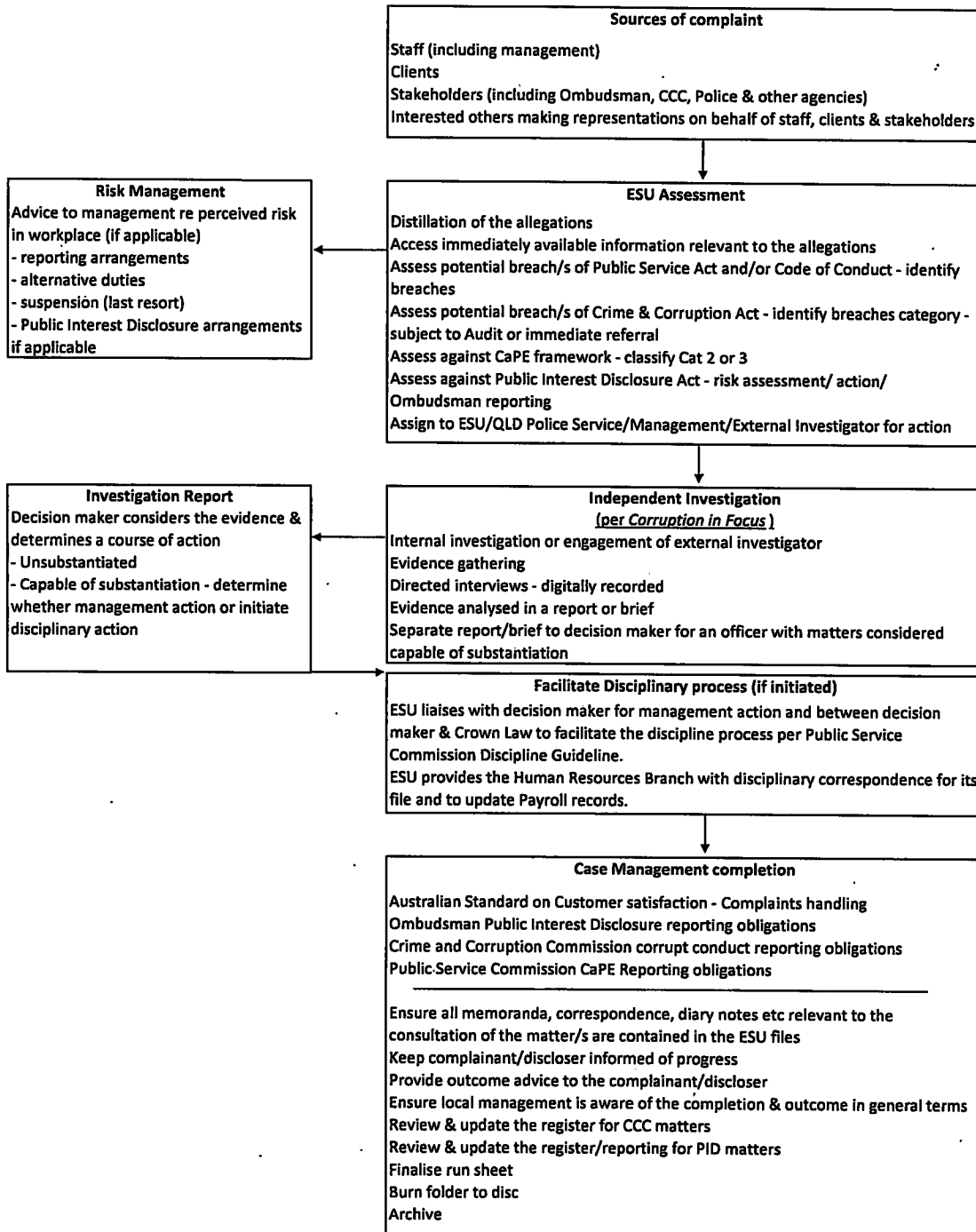
## DJAG Corrupt Conduct & Misconduct Case Management Flowchart

*"The Executive Director, Ethical Standards Unit, is involved in the development and delivery of programs to improve ethical culture and ethical decision making across DJAG; manages the investigation of allegations of misconduct and corrupt conduct and the submission of reports and advice to decision makers involving serious workplace conduct and disciplinary issues.*

*Allegations of misconduct and corrupt conduct are to be referred to the Executive Director immediately.*

*The Executive Director is also the Crime and Corruption Commission Liaison Officer and Public Interest Disclosure Officer."*

DJAG Intranet



Approved ☒ Not Approved ☐  
Signed:   
David Mackie  
Director-General  
Department of Justice and Attorney-General  
Date: 20.5.19

Department of Justice and Attorney General

Information Technology Services

# Use of ICT Services, Facilities and Devices Policy

## Document information

Security classification	UNCLASSIFIED		
Date of review of security classification	June 2017		
Authority	Executive Director, Information Technology Services		
Documentation status	Final	Consultation release	<input checked="" type="checkbox"/> Final version
Next review date	June 2019		
Document reference	eDOCS number: 3711798		

## Version history

Version	Notes	Author	Date of change
1.0	Approved by IMC as the Information Management Branch's Use of Information and Communication Technology (ICT) Devices Policy	-	March 2005
2.0	Changed to IMB Policy Template and minor editing amendments that do not change context of document	Terry McDonald	July 2005
3.0	Review, update and major change of policy – merging telecommunications, BlackBerry and ICT devices and facilities into one policy.	Marija Mamic	March 2007
4.0	Full redraft covering latest QGCIO IS38 update, currency for DJAG, comparison to other state government department published policies and increased definition and examples on misuse of information and Authorised/Unauthorised use.	Raamon Vaccaro	June 2016
5.0	Further update and review from consultation.	Brenda Lee	12 July 2016
6.0	Final version replaces all previous versions of the Information Management Branch's Use of Information and Communication Technology (ICT) Devices Policy, and Information & Communication Technology Branch's Internet and Email Usage Standards.	Brenda Lee	23 January 2017
7.0	Amendment to include DG directive to reflect usage of private email accounts should not to be used for government purposes, as documents may constitute records under public records act	Peter Waye	28 September 2017

## Policy owner/enquiries

Direct all enquiries and assistance regarding use of ICT services, facilities and devices, including any suggested updates and changes to this policy to the Justice IT Service Desk on 3239 0001 or by email [justiceitservicedesk@justice.qld.gov.au](mailto:justiceitservicedesk@justice.qld.gov.au).

This policy is owned by the Executive Director, ITS, who is responsible for the development and ongoing review of the policy.

## Policy approval and review

This policy was endorsed by the departmental Information and Technology Innovation Committee (ITIC) on 8 June 2017.

This policy was approved by David Mackie, Director-General, Department of Justice and Attorney-General on 13 July 2017.

---

The Executive Director, Information Technology Services, Department of Justice and Attorney-General is responsible for the development and ongoing review of this policy.

This policy will be reviewed at least every two years. The next scheduled review is June 2019.

### **Security classification**

This document has a security classification of UNCLASSIFIED.

### **License**

Use of ICT services, facilities and devices policy © The State of Queensland (Department of Justice and Attorney-General) 2017.



<http://creativecommons.org/licenses/by/4.0/deed.en>

This work is licensed under a Creative Commons Attribution 4.0 International Licence. You are free to copy, communicate and adapt this work, as long as you attribute by citing 'Use of ICT services, facilities and devices policy, State of Queensland (Department of Justice and Attorney-General) 2017'.



---

## 1. Purpose

This policy addresses employee use and the monitoring of ICT services, facilities and devices with the Department of Justice and Attorney-General (DJAG). It will:

- set clear expectations for employees on what the department considers appropriate and authorised use of ICT services, facilities and devices, and
- ensure ICT services, facilities and devices are used by employees in a manner that is efficient, effective, minimises risks and can survive public scrutiny and/or disclosure<sup>1</sup>.

This policy supports the Queensland Government Chief Information Office's Use of ICT services, facilities and devices policy - IS38 and Public Service Commission's (PSC) Use of internet and email policy.

## 2. Applicability

This policy applies to all ICT services, facilities and devices (owned, leased or licensed), provided to employees to carry out their work, regardless of their location (online, in Australia or overseas).

For the purposes of this policy, employee refers to all DJAG staff, including temporary staff, contractors and consultants and any other person who provides a service on a paid or voluntary basis to DJAG.

## 3. Policy statement

The department provides employees with ICT services, facilities and devices on the basis they are used for activities defined in accordance with authorised use in section 5 this policy and legislative requirements, including the:

- Code of Conduct for the Queensland Public Service (Code of Conduct)
- *Public Sector Ethics Act 1994 (Qld)*
- *Public Service Act 2008 (Qld)*.

All employees are accountable for their actions while using departmental ICT services, facilities and devices, and must abide by the roles and responsibilities contained in section 9 of this policy.

Any use of ICT services by employees must:

- be able to withstand internal and public scrutiny and/or disclosure, and
- respect the dignity, rights and views of others.

Work documents, data, messages, email, correspondence and information created, received and/or stored on departmental devices or through other ICT facilities or services may constitute public records under the Public Records Act 2002 (Qld) and/or be subject to disclosure under the Right to Information Act 2009 (Qld), the Information Privacy Act 2009 (Qld) or subpoena.

The department has adopted a zero tolerance approach to the misuse / inappropriate use of its ICT services, facilities and devices.

The department will periodically review, assess and address any risks associated with the use of ICT services, facilities and devices and take appropriate action as needed.

The department will educate and inform employees on the use of ICT services, facilities and devices including their responsibilities<sup>2</sup> as set out in this policy.

---

<sup>1</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Policy benefits

<sup>2</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Requirement 2 and PSC's Use of internet and email policy, Principle 7.6

---

## 4. Provision and ownership

The department provides and/or allows devices be used to access the department's systems, software and other facilities and services.

### ***Departmental ICT devices***

ICT devices wholly purchased by the department are public resources and must be properly maintained, managed and protected against theft and damage. When managing ICT devices Information Technology Services Branch (ITS) under authorisation processes may remotely remove any departmentally provisioned service and associated data through these devices. This remote access may inadvertently remove an employee's limited personal data/information.

### ***Employee's personal ICT devices<sup>3</sup>***

An employee owned ICT device can access departmental email, OneDrive, calendar services through Office 365 and other Office 365 applications by using an ITS approved remote access solution. Other departmental ICT applications and services are **not** sanctioned for use on personal devices.

When accessing departmental information from a personal device, employees should ensure that they:

- understand they are responsible for any service billing or other financial charges associated with the device
- understand that the department will not assist in any issues relating to the device
- do not compromise the department's information security
- abide by authorised use requirements within this policy when using departmental ICT facilities and services and handling departmental information
- ensure only PUBLIC, UNCLASSIFIED and X-IN-CONFIDENCE information is created or used within the device
- understand that in the event of security breaches ITS may remotely wipe a departmentally approved system or program that has been implemented under a departmental licence or agreement, and in doing so the department may inadvertently remove their personal information.

Employees must remove departmental information from their personal device and cease accessing the department's services on the device:

- when it is no longer required for departmental work purposes
- upon leaving the employment of the department
- before any exchange of the equipment such as under warranty or for repair, or
- before disposal of the device.

While the department applies a range of security controls, it makes no warranties that access to the department's ICT services and facilities will be continuous, fault-free or secure. The department does not accept responsibility for any loss of personal data, delays, non-deliveries, service interruptions, technical difficulties or malicious activity arising, whether directly or indirectly, out of an employee's use of the department's ICT services and facilities on their own device.

## 5. Authorised use<sup>4</sup>

Using the department's ICT services, facilities and devices is authorised for the purposes of:

- a) conducting official business in pursuit of departmental objectives which means:

---

<sup>3</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Implementation guideline section 4.1

<sup>4</sup> QGCIO Use of ICT services, facilities and devices policy – IS38, Requirement 1, PSC's Use of internet and email policy and Principles Statement, Principles 7.2 and 7.3

- 
- i. accessing and/or using ICT services, facilities and devices and information specifically for work related purposes
  - ii. communicating with colleagues, external stakeholders or partners, on work related matters
  - b) supporting professional development, as approved by the employee's manager or supervisor, such as:
    - i. professional development relating to study or research in accordance with the department's Study and Research Assistance Scheme (SARAS) Policy
    - ii. approved forum, conference or seminar participation
    - iii. engaging with a professional or industrial organisation for membership, registration, training/education, performance, conduct or safety
  - c) undertaking work related to the Armed Forces (Reserve)
  - d) limited personal use.

When using departmental ICT services, facilities and devices, employees are also subject to the following conditions and must:

- prior to the access/use of any ICT services, facilities and devices read and acknowledge any terms and conditions provided
- follow any conditions of use
- not attempt to disable, prevent or circumvent any existing or future security measures
- not share their logon (user ID) and password information, and will be held personally responsible for any activity that has taken place by not managing their logon
- take all necessary precautions to prevent unauthorised use or theft including not leaving devices in an unlocked or unattended state
- comply with the PSC's Use of internet and email policy
- manage records in accordance with the department's Recordkeeping policy
- protect personal information in accordance with the Information Privacy Act 2009 (Qld)
- determine the information security classification of the information and protect it according to the applicable controls
- protect intellectual property including copyright
- respect the dignity, rights and views of others when communicating
- only use software or online services which has been authorised or purchased through ITS
- abide by software licenses, copyright including Creative Commons licences (AusGOAL) and any intellectual property requirements they use
- seek prior approval from their manager or supervisor before taking a departmental ICT device overseas and/or enabling international roaming.

See Attachment 1: Definitions for examples of authorised use.

### ***Limited personal use***

Limited personal use of ICT services, facilities and devices by employees means that it:

- a) incurs minimal additional expense, does not interfere with and does not affect the business activities of the department
- b) is brief and infrequent
- c) is not for or in connection with private business
- d) is able to withstand scrutiny of colleagues, the community and media
- e) does not unnecessarily impact on an employee's ability to undertake their duties
- f) is consistent with this policy and the Public Service Act 2008 and/or the Code of Conduct and does not violate any other departmental policy and state or Commonwealth policy, legislation or regulation regarding the use of ICT services, facilities and devices.

---

The department provides a personal drive (OneDrive or equivalent) for the storage of personal, ephemeral and reference information. It is the employees responsibility to ensure that any personal data/information is backed up and that these work related storage areas are not used as the primary location to store personal data.

Information and usage associated with limited personal use is also subject to the same access, retrieval, review and monitoring practices as employment related use and is subject to the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld).

The department does not accept liability for any loss or damage suffered as a result of an employee using departmental ICT services, facilities and devices for personal use.

Personal use of the department's ICT services, facilities and devices can be revoked at any time.

See Attachment 1: Definitions for examples of limited personal use.

Where employees have any doubt as to what is authorised use or limited personal use, must discuss this with their manager or supervisor.

## 6. Unauthorised use<sup>5</sup>

Access or use of any ICT services, facility or device that does not meet the conditions of authorised use will constitute unauthorised use, which is a manner that is inappropriate or unlawful by:

- a) failing to behave in a manner which supports the Public Service Act 2008 (Qld), the Code of Conduct, the Use of internet and email policy, this policy and other departmental policies and associated legislation (see **Attachment 2: References**)  
Private email accounts (or communication services such as text messages) should not be used for government-related business.
- b) misusing information from departmental systems, including:
  - i. accessing departmental business information and systems without an authorised business purpose (e.g. emailing departmental documents to a personal email account for unauthorised purpose, selling information for personal profit, searching classified information to share with a friend, acquaintance or family member)
  - ii. searching records, including client records, on a departmental database without an authorised business purpose (for clarity this means that staff members are not permitted to browse client files for their own interest unless the staff member has a specific work related requirement to view those records. Additionally, it is not appropriate in any circumstance for staff members to view records of client/s that are known to them on a personal basis)
  - iii. distributing information from departmental business systems to the public or media
  - iv. handling classified information inappropriately
  - v. extracting, disclosing, modifying, adding or deleting business information when not for a departmental purpose.

The PSC's Use of internet and email policy provides the consequences should an employee inappropriately uses the internet or email.

See Attachment 1: Definitions for examples of unauthorised use.

Where employees have any doubt as to what is unauthorised use, employees must discuss this with their manager or supervisor.

---

<sup>5</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1

---

## 7. Accessing, monitoring and restrictions

The department logs and monitors departmental services on a daily basis using ICT networks, operating systems, applications, web servers, mail servers, gateways, log transactions and communications. Scanning occurs by virus protection software on any ICT device (personal or not) that is connected to the department's network such as a USB key. Monitoring may also occur at the manager or supervisor level for licenses, internet and printer usage, and access to systems to evaluate optimisation and cost efficiencies.

Incoming and outgoing email (including emails of a personal nature), and their attachments, are automatically scanned for the detection of viruses, suspect or malicious code, SPAM, executable programs, unacceptable size and unacceptable content. Emails that represent a clearly defined security or maintenance threat to the department's ICT network are automatically quarantined with a simultaneous notification message sent to the intended recipient. Suspect emails are kept for 30 days and thereafter automatically deleted.

To access ICT services or facilities from a non-corporate ICT device additional security may need to be established. This may include the use of an employee's personal mobile number in order to provide a security access code.

All actions regarding the use of ICT services, facilities and devices (including those of a personal nature) are legally a public record of government business. All use may be monitored, audited, recorded and reviewed for compliance with departmental policies, standards, legislation and Code of Conduct. Relevant information is disclosed with authorisation as deemed appropriate in the circumstances.

## 8. Non-compliance with this policy

The department will manage all alleged breaches of this policy in accordance with Public Service Act 2008 (Qld) and the Code of Conduct. Employees breaching this policy may be subject to disciplinary action (including termination of employment) subject to the principles of natural justice.<sup>6</sup> A pattern of behaviour (e.g. repeated use) will be a factor for consideration in determining the penalty.

## 9. Roles and responsibilities

### ***Employees***

All employees (see Attachment 1: Definitions) are responsible for:

- reporting lost, stolen or damaged ICT devices
- only using ICT services, facilities and devices for activities as defined in authorised use
- reporting instances of unauthorised use
- keeping the credentials of ICT systems secure (including user ID and passwords)
- returning departmental software and devices upon ceasing employment with the department
- protecting software or devices against theft and damage
- managing departmental information in accordance with the Information security policy and the Recordkeeping policy
- seeking clarification on this policy if they do not understand what is required of them.

Where an employee has any doubts about what is required of them, they must discuss with their manager or supervisor in the first instance. If further clarification is required, contact the Justice IT Service Desk.

---

<sup>6</sup> PSC's Use of internet and email policy, Principle 7.5

---

## ***Managers or supervisors***

Managers or supervisors (see Attachment 1: Definitions), or their delegate, are responsible for:

- ensuring ongoing staff educating/awareness of this policy, including during induction
- notify the Justice IT Service Desk of employees ceasing employment or beginning long term leave /secondment from the department
- regularly reviewing employee access to ICT services, facilities and devices so that it is commensurate with the role being performed
- ensuring employees receive sufficient education to use the department's ICT services, facilities and devices
- ensuring all ICT purchases are made through ITS or with their approval in accordance with the Financial Management Practice Manual.

## ***Chief Information Officer and Information Technology Services, Corporate Services***

Information Technology Services (ITS), Corporate Services is responsible for:

- developing, maintaining and communicating this policy
- endorsing ICT purchases for the department as per Financial Management Practice Manual (Section 11.1.13)
- keeping scanning and monitoring software to ensure legislative and departmental policy requirements are met, with guidance and/or direction from the Executive Director, Human Resources, Director, Legal Advice and Advocacy, the Assistant Director-General Corporate Services, Ethical Standards Unit and/or Internal Audit, as required.

The Chief Information Officer is responsible for authorising:

- the monitoring of ICT services, facilities and devices
- access, retrieval and review of information and records from or related to ICT services, facilities and devices
- any investigation or inquiry being carried out by Ethical Standards Unit, Internal Audit or a manager.

## ***Director-General***

The Director-General or delegate is responsible for determining whether a breach of this policy has occurred and undertaking the appropriate course of action e.g. disciplinary action.

## **10. Reporting requirements**

Internal Audit may conduct audit reviews of ICT information systems (including system logs) to assess compliance of procedures, practices, behaviours, legal and administrative requirements. Details of employees disciplined for breaches of this policy and/or PSC's Use of internet and email policy subject to mandatory reporting requirements, may be referred to relevant law enforcement and/or oversight body (such as the Crime and Corruption Commission).



## Attachment 1: Definitions

For the purpose of this policy, the following definitions shall apply:

Term	Explanation
Authorised use <sup>7</sup>	<p>Authorised use of departmental ICT services, facilities and devices is restricted to the following activities:</p> <ul style="list-style-type: none"> <li>a) official business</li> <li>b) professional development</li> <li>c) armed forces related work, and</li> <li>d) limited personal use.</li> </ul> <p>For a more detailed explanation see section 5.</p> <p><b>Examples of <i>Authorised use</i> include but not limited to:</b></p> <ul style="list-style-type: none"> <li>• printing documents relating to a departmental training course</li> <li>• using the internet to perform departmental related case/project research</li> <li>• using email to communicate new departmental directives or policies</li> <li>• informing employees of new departmental initiatives and/or staff movements</li> <li>• placing a telephone call to other government agencies for the purpose of acquiring or sharing information.</li> </ul>
Blog	A web log usually set up as a personal journal that is publicly accessible.
Code of Conduct for the Queensland Public Service (Code of Conduct)	<u>Code of Conduct for the Queensland Public Service</u> sets out standards of behaviour for all Queensland public service agency employees, contractors, subcontractors (including employees of contractors and subcontractors), students and volunteers who work in any capacity for a Queensland public service agency.
Department	Department of Justice and Attorney-General
Digitisation	The creation of digital images from paper documents by such means as scanning or digital photography. <sup>8</sup>
DJAG	Department of Justice and Attorney-General
Employee	For the purposes of this policy, employee refers to all departmental staff, including temporary staff, contractors and consultants and any other person who provides a service on a paid or voluntary basis to the department. It excludes Judicial Officers and Judicial Associates, who are not public servants, are exempt from the requirement to abide by this policy.
Ephemeral information	Ephemeral documents are items of short-term temporary information value.
ICT	Information and communication technology
ICT devices	<p>Electronic equipment designed for a particular communication and/or function, including but not limited to:</p> <ul style="list-style-type: none"> <li>• computers (e.g. desktop computers, mobile devices, laptops, servers, consoles and handheld devices)</li> <li>• phones (including fixed lines, mobiles, smart phones and satellite telephones) and accessories to phones (including battery chargers, cables)</li> <li>• digital or analogue recorders and removable media (e.g. USBs, DVDs, video, portable hard drives)</li> <li>• radios or other high frequency communication devices</li> <li>• televisions, computer monitors and videoconferencing equipment</li> </ul>

<sup>7</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1 and Authorised and unauthorised use of ICT services, facilities and devices guideline.

<sup>8</sup> Queensland State Archives - Digitisation Disposal Policy, Policy for Queensland Public Authorities, August 2014



Term	Explanation
	<ul style="list-style-type: none"> <li>digital or analogue players/recorders (including DVD and video), cameras</li> <li>monitors and sensors</li> <li>printing, photocopying, facsimile, scanning machines and multi-function devices.</li> </ul>
ICT facilities	A telecommunication service designed for a particular communication and/or function, which includes but is not limited to IT networks and servers, IT systems, wireless networks, internet, extranet, email, instant messaging, webmail, fee-based web services and social media.
ICT services	Telecommunications or transmission services that carry voice and/or data and includes applications, hosting, storage, online services delivered over the web and cloud based services etc. The services includes software generally e.g. core business application, Microsoft suite of products such as the Office 365 service, and operating software on computers or servers.
ICT services, facilities and devices	See ICT services, ICT facilities and ICT devices within this definition attachment.
Information security classification	Information is classified according to the nature of the information and the possible damage it may cause for example, PUBLIC, UNCLASSIFIED or IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED. QGCIO's Information standard - IS18 mandates that all agency information assets are assigned appropriate classification which then determines the appropriate controls to handle those information assets <sup>9</sup> .
Intranet	The internal website usually accessed by a web-browser that is accessible by the department only, as it is restricted by a firewall.
IS	Queensland Government Chief Information Office's Information Standard.
ITS	Information Technology Services, part of the Corporate Services Division within the department.
Limited personal use	<p>Personal use of departmental ICT services, facilities and devices by employees means be brief, infrequent and at minimal cost to the department. For a more detailed explanation see Section 5.</p> <p><b>Examples of authorised limited personal use include but not limited to:</b></p> <ul style="list-style-type: none"> <li>using the internet to access a news website</li> <li>using a printer or photocopier to print out a few pages of personal information on limited occasions</li> <li>making or receiving brief local telephone calls, or sending mobile phone SMS messages, to a partner/friend in relation to work, family or other personal commitments</li> <li>using a fax or email to change personal banking details</li> <li>making financial transactions, including bill paying, home banking and purchasing non-work related goods and services which do not relate to a personal private business</li> <li>for those employees working offsite from departmental premises and away from home, using their personal email on a departmental device in order to manage personal affairs.</li> <li>completing a job application</li> <li>printing and distributing information relating to professional training/seminar events</li> <li>conducting searches over the internet on appropriate and ethical topics that will not cause embarrassment or harm to the department</li> <li>reading personal internet based email is open to scrutiny and must not be inappropriate, unlawful or criminal and does not relate to a private business enterprise.</li> </ul>

<sup>9</sup> Queensland Government's Information Security Classification Framework.

Term	Explanation
	<p><b>Examples of unauthorised limited personal use include:</b></p> <ul style="list-style-type: none"> <li>• using a departmental telephone to call overseas telephone numbers for personal reasons where it is not an emergency situation</li> <li>• making personal phone calls or electronic communications of long duration</li> <li>• sending emails of a personal nature via a group distribution list without appropriate approval</li> <li>• using the departmental telephones, meeting room or videoconferencing facilities to conduct personal conference calls</li> <li>• using departmental photocopiers and/or printers to photocopy/print out a large amount of personal information such as flyers for a school fete</li> <li>• using governmental ICT equipment to express political views, whether utilising a government email account or a personal email account (e.g. via Gmail)</li> <li>• using your government email account to contribute to non-work-related online feedback forums, voting online or blog sites, or to submit personal comments online in response to current issues.</li> </ul>
Manager or supervisor	A role within the department that has responsibility, either directly or indirectly, of an employee.
Metadata	Data that describes other data. For example, recordkeeping metadata is information describing the context, content and structure of records and their management. Metadata allows for information management, such as improving search ability.
Monitoring	The process of checking, observing, tracking, recording and/or evaluating employees use of the department's ICT services, facilities and devices.
Non-corporate ICT device	Any ICT device not purchased or managed by the department to enable an employee to perform their work duties.
Online service	Use of the internet for information service delivery and/or collaboration with other government agencies and organisations external to the department.
Phishing	The act of sending an email to a user falsely claiming to be an established legitimate enterprise, in an attempt to induce the user into surrendering private information for an unlawful activity such as identity theft.
Policy	This Use of ICT services, facilities and devices policy document.
Public Safety Network (PSN)	A secure Queensland Government data network infrastructure that includes DJAG, Queensland Corrective Services, Queensland Police, Rural Fire, Queensland Ambulance and Queensland Fire.
Public service employee	A person employed under the <i>Public Service Act 2008 (Qld)</i> in agencies, departments or public service offices.
QGCIO	Queensland Government Chief Information Office.
Record	Records are recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the public authority's business or affairs. In the context of business systems, a record could be an entire business system, a row in a table or an extract of data in the form of a report <sup>10</sup> .
RDS	Remote desktop service.
Scanning and monitoring software	Software that monitors and tracks elements within or that pass through a computer network.
Spam	Unsolicited 'junk' email sent to large numbers of people, often from automated systems, to promote products or services.

<sup>10</sup> Queensland State Archives - Website [glossary](#)

Term	Explanation
Spyware	Any software that covertly gathers user information through the user's internet connection without his or her knowledge. Spyware is often used for advertising purposes and a spyware application is typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses, passwords and credit card numbers.
Trojan horse	A destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive.
Unauthorised use <sup>11</sup>	<p>Access or use of any ICT service, facility or device that does not meet the conditions of authorised use will constitute unauthorised use, which is a manner that is inappropriate or unlawful. Examples of unauthorised use include but limited to:</p> <ul style="list-style-type: none"> <li>a) downloading, storing or distributing pornography using departmental ICT services, facilities and devices</li> <li>b) taking inappropriate and/or pornographic pictures with a mobile phone camera or any other form of camera or portable device</li> <li>c) forwarding inappropriate jokes and graphics, particularly any material of a sexually explicit, racist, defamatory, indecent, obscure, profane or offensive nature</li> <li>d) maintaining or supporting a personal private business (including your own business or a family/friend's business), including fee-based or subscription services or stock trading</li> <li>e) creating or maintaining personal websites</li> <li>f) knowingly accessing or downloading website material that is defamatory, harassing or discriminatory or sending messages that are defamatory, harassing or discriminatory</li> <li>g) online gambling, stock trading or accessing dating services online</li> <li>h) downloading image/sound/movie files and records, such as photos, .mp3, .wav and .avi files or similar files in other formats, unless for official business purposes</li> <li>i) sending and/or downloading material such as chain letters or letters relating to pyramid schemes or in any way participating in such activities</li> <li>j) disrupting the department's ICT services, facilities and devices such as spamming or other forms of mass mailing, storing and/or transmitting large files or any other unnecessary activity that may place a burden on departmental resources</li> <li>k) knowingly downloading, sending and/or broadcasting material from the internet or email containing viruses, worms, time bombs, cancel bots, Trojan horses, spyware or any other contaminating or destructive features</li> <li>l) knowingly accessing internet sites and activities which a reasonable person would find offensive in the workplace or contain unlawful practices (e.g. bomb making instructions), except where related to an approved genuine departmental business requirement</li> <li>m) installing software on departmental ICT devices without firstly obtaining the approval from the manager or supervisor</li> </ul>

<sup>11</sup> QGCIO's Use of ICT services, facilities and devices policy – IS38, Requirement 1 and Authorised and unauthorised use of ICT services, facilities and devices guideline.

Term	Explanation
	<p>n) installing departmentally provisioned software on ICT devices personally owned by the employee, or installing instances of software where licensing isn't departmentally provisioned</p> <p>o) accessing, playing and/or distributing computer games or unlicensed software</p> <p>p) accessing internet streaming services, such as radio and television, video streams, sports broadcasts, simulcasts on any departmental owned ICT services, facilities and devices, except where related to an approved departmental business or education requirement</p> <p>q) accessing ICT services such as online chat and info call services (e.g. 1900 telephone numbers), unless for work purposes</p> <p>r) posting messages representing the department on the internet and/or any other public computer system without first obtaining the approval of a manager or supervisor</p> <p>s) representing personal opinions on the internet/email as those of the department, or otherwise failing to comply with departmental practices concerning public statements about the government's position</p> <p>t) transmitting proprietary information or confidential information related to clients, suppliers, vendors or trading partners (e.g. via email or other internet services)</p> <p>u) failing to comply with confidentiality agreements with third parties that may explicitly prohibit communication over public computer systems</p> <p>v) failing to keep secure the department's ICT system and software access 'logins' (user name) and passwords issued to employees, including the transmission of this information over the internet and/or via email accounts</p> <p>w) engaging in any form of phishing or obscuring the origins of any message or download material under an assumed internet address or otherwise disguise a user's identity</p> <p>x) altering the content of an email received without the sender's approval or without clearly indicating that you have altered the content</p> <p>y) infringing intellectual property rights of others (e.g. copying or downloading video or software where copyright does not permit) or unlawfully circumventing technological protection measures designed to deter copyright infringement</p> <p>z) deliberately misusing and/or not taking due care of departmental ICT devices</p> <p>aa) failing to adhere to safety requirements and restrictions on usage of devices (e.g. failing to adhere to mobile phone usage restrictions in designated hospital areas, failing to take care and/or using hands-free communication equipment when using a mobile phone whilst a vehicle is moving)</p> <p>bb) stealing departmental ICT services, facilities and devices and/or information</p> <p>cc) allowing unauthorised persons, whether external (e.g. friends or relatives) or internal to the department, to use the department's ICT services, facilities and devices</p> <p>dd) using ICT services, facilities and devices and/or departmental information in a way which waives or has the potential to waive the department's legal professional privilege in the contents of legal advice</p> <p>ee) private email accounts (or communication services such as text messages) should not be used for <u>government-related business</u>.</p> <p>For a more detailed explanation, see Section 6.</p>

---

Term	Explanation
Virus	A computer program or piece of code that embeds into your computer files without your knowledge and runs against your wishes. Most viruses can also replicate themselves and spread to other computers. All computer viruses are man-made usually for malicious intent.
Worm	A computer program capable of reproducing itself that can spread from one computer to the next over a network. Worms take advantage of automatic file sending and receiving features found on many computers.

---

## Attachment 2: References

The requirements set out in this document are based on, and are consistent with, relevant government legislation, regulations, directives, information standards and/or policies at the time of publication.

### Departmental policies and procedures

Recordkeeping Policy

Information security policy

Information Security Plan

Financial Management Practice Manual

IT Equipment Collection & Disposal Form

### Queensland Government policies

Code of Conduct for the Queensland Public Service

Queensland Government Chief Information Office's Use of ICT services, facilities and devices policy – IS38

Public Service Commission's Use of Internet and email policy

Queensland Government Chief Information Office's Information Security – IS18 Information Standard

Queensland Government information security classification framework

Crime and Corruption Commission's Confidential information: unauthorised access, disclosure and the risks of corruption in the Queensland public sector

### Legislation and regulations

Crime and Corruption Act 2001 (Qld)

Information Privacy Act 2009 (Qld)

Public Sector Ethics Act 1994 (Qld)

Public Service Act 2008 (Qld)

Right to Information Act 2009 (Qld)

Public Records Act 2002 (Qld)

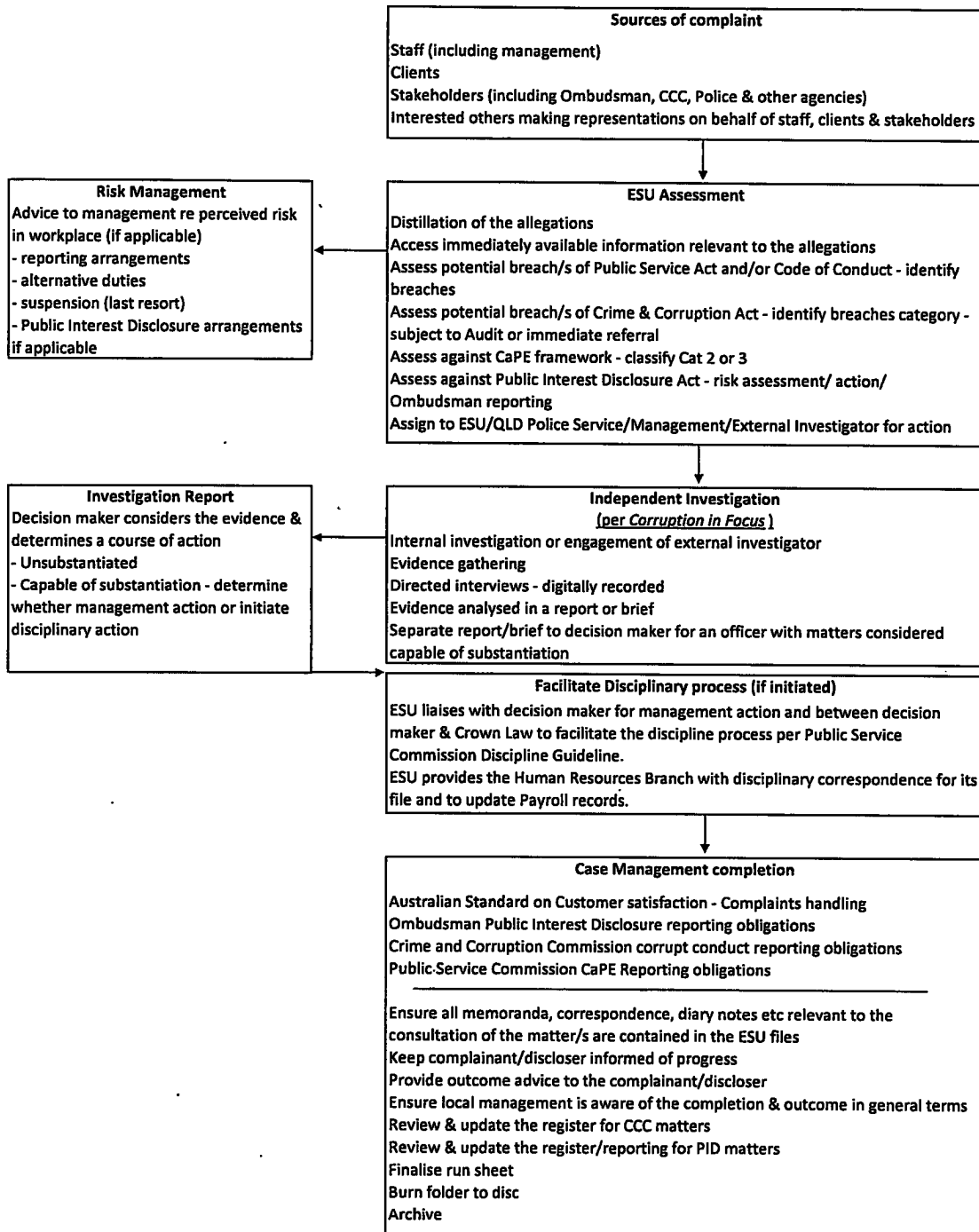
## DJAG Corrupt Conduct & Misconduct Case Management Flowchart

*"The Executive Director, Ethical Standards Unit, is involved in the development and delivery of programs to improve ethical culture and ethical decision making across DJAG; manages the investigation of allegations of misconduct and corrupt conduct and the submission of reports and advice to decision makers involving serious workplace conduct and disciplinary issues.*

*Allegations of misconduct and corrupt conduct are to be referred to the Executive Director immediately.*

*The Executive Director is also the Crime and Corruption Commission Liaison Officer and Public Interest Disclosure Officer."*

DJAG Intranet



Approved ☒ Not Approved ☐  
Signed:   
David Mackie  
Director-General  
Department of Justice and Attorney-General  
Date: 20.5.19



## Ethical Standards Unit

# Dealing with allegations of corrupt conduct and misconduct

### Purpose

The Department of Justice and Attorney-General (DJAG) is committed to the timely resolution of complaints of alleged corrupt conduct and misconduct. This policy and associated procedures/templates exist to outline how the Ethical Standards Unit (ESU) deals with allegations of corrupt conduct and misconduct. A detailed flowchart is attached (**Attachment 1**), which also details the process outlined in this policy, which was approved by the Director-General, Department of Justice and Attorney-General.

The Executive Director, ESU is involved in the development of programs to improve culture and ethical decision making across DJAG; manages the investigation of allegations of misconduct and corrupt conduct and the submission of reports and advice to decision makers involving serious workplace conduct and disciplinary issues.

### Misconduct, corrupt conduct and Public Interest Disclosures

Employee complaints about corrupt conduct or misconduct are managed by the ESU in accordance with *Crime and Corruption Act 2001*, *Public Sector Ethics Act 1994* and *Public Service Act 2008*.

**Corrupt conduct** – is conduct by any person, regardless of whether they are a public sector employee, which meets all elements of either **Type A** or **Type B**:

**Type A** [s15(1)] is conduct by any person which meets all 3 tests of:

- a) Adversely affects, or could adversely affect performance of functions or the exercise of powers of a unit of public administration; or a person holding an appointment; **AND**
- b) Results, or could result in conduct which is not honest or is not impartial; or involves a breach of trust; or involves a misuse of information or material acquired; **AND**
- c) Would, if proved, be a criminal offence; or a disciplinary breach providing reasonable grounds for terminating the person's services.

**Type B** [s15(2)] is conduct by any person which meets all 3 tests of:

- a) Impairs, or could impair, public confidence in public administration; **AND**



b) Involves, or could involve, any of the following;

- collusive tendering;
- fraudulent applications for licences, permits and other authorities under an Act necessary to protect the health and safety of persons, the environment, the use of the State's natural resources;
- dishonestly obtaining benefits from the payment or application of public funds or the disposition of state assets;
- evading State taxes, levies, duties or fraudulently causing a loss of State revenue;
- fraudulently obtaining or retaining an appointment; **AND**

c) If proved, would be a criminal offence; or a disciplinary breach providing reasonable grounds for terminating the person's services if they were (or are) an appointment holder.

*Please note:* Each case needs to be assessed on its own merits as to whether it constitutes corrupt conduct. The Department has an obligation to notify the Crime and Corruption Commission (CCC) if corrupt conduct is reasonably suspected, subject to reporting arrangements with the CCC (e.g. S.40 Directions).

**Misconduct** – is inappropriate or improper conduct in an official capacity; or inappropriate or improper conduct in a private capacity that reflects seriously and adversely on the public service.

Examples of conduct which might constitute corrupt conduct or misconduct include:

- failing to declare a conflict of interests
- using alcohol, drugs or other substances in a way that adversely affects performance
- excessive use of internet for personal amusement or other unauthorised purposes
- insulting or swearing at clients, customers or colleagues
- victimising another public service employee
- accessing inappropriate material on the internet (e.g. pornography) emailing or storing it
- unauthorised personal use of departmental cars, fuel cards, taxi vouchers or information
- stealing money or equipment
- using authority of a role for personal gain
- cheating on travel allowances
- compromising a selection process
- sexual harassment
- workplace harassment

Allegations of corrupt conduct and misconduct are to be referred to the Executive Director, ESU immediately.

The Executive Director is also the Crime and Corruption Commission Liaison Officer and Public Interest Disclosure Co-ordinator.

Complainants of suspected corrupt conduct may be protected under the Public Interest Disclosure Act 2010 (see Public Interest Disclosure (PID) Policy).

## **Case Management**

### **Receiving complaints**

The ESU receives complaints of alleged corrupt conduct and misconduct from a range of sources, including staff (including management), clients (including prisoners and youth in detention), stakeholders (including the Office of the Queensland Ombudsman, the CCC, Police and other agencies) and interested others making representations on behalf of staff, clients and stakeholders.

When a complaint is received the matter is allocated to an Ethics Consultant to complete an assessment of the allegations and suggest an appropriate course of action.

### **Assessment**

The ESU completes a detailed Complaint Assessment form (see *00 - Complaint Assessment Form – v6*). The Complaint Assessment form details all relevant complaint information; assesses possible breaches of policies; distils allegations; assesses whether the alleged conduct has the characteristics of corrupt conduct under the *Crime and Corruption Act 2001*, or whether the alleged conduct would amount to a Conduct and Performance Excellence (CaPE) matter; assess if the alleged conduct is a PID; and outlines the recommended course of action.

The Complaint Assessment form and recommended course of action is approved by the Executive Director, ESU. ESU ensure that all Complaint Assessments are completed in a timely manner and when possible within 2 business days of receiving the complaint.

In certain circumstances, a complaint may not progress further than a Complaint Assessment form as no further action is required by ESU. In these circumstances, the ESU should write to the complainant to advise them that no further action will be taken in relation to their complaint and outline the reasons why.

In the Complaint Assessment stage, a complaint may be deemed suitable for divisional action, which assigns responsibility of investigation or other action in relation to the allegation, to the division involved. The divisional action process is outlined in the divisional action templates (see *17 - Divisional Action Form – v3*).

Local enquiries should be conducted in accordance with the Public Service Commission's Managing Workplace Investigations Guide.

### **Risk Management**

As part of the assessment process, the ESU undertakes a risk management assessment in relation to any perceived risks in the workplace relating to the complaint. Some options that are taken into consideration include reporting arrangements, alternative duties and suspension, which is a last resort. If the ESU considers such action is warranted, the ESU will provide this advice to the relevant delegated

decision-maker. Additionally, if the complaint is assessed as a PID, the ESU completes a PID disclosure form, which includes a separate PID Risk Assessment (see 12 - **PUBLIC INTEREST DISCLOSURES Reporting – v5-2**).

## **Independent Investigation**

If it is determined that an independent investigation is warranted, the ESU undertakes an investigation in accordance with the CCC's Corruption in Focus. In some circumstances, the ESU will engage an external investigator to undertake an independent investigation on the Department's behalf.

The investigation involves gathering evidence from a range of sources, which may include interviewing relevant parties and analysing the evidence gathered in a report and/or memorandum.

Any person being interviewed as part of an ESU investigation is generally provided with written notification of the interview, allegations and are requested (if not an employee) or directed (if an employee) to participate in an interview. The interviews are electronically recorded to ensure an accurate record on the interview. The ESU encourages interviewees to have a support person present (see 10 - **Support person - Fact Sheet - v2**) and provide the contact details for the Employee Assistance Program (EAP) for staff.

## **Safety**

Safety of ESU staff must be considered during the conduct or case management of investigations. In circumstances where risk may arise, e.g. attending a client or officer's home or interviewing someone known to be violent, a second ESU staff member should assist and any other risk management taken as determined appropriate in consultation with the Executive Director.

## **Investigation Report**

If an investigation is conducted, the Ethics Consultant or the external investigator completes a detailed investigation report (see 15 - **Investigation Report - Template - v2e**).

The report outlines all of the evidence gathered and the investigator will conclude whether they consider the allegation/s capable of substantiation. This allows the decision-maker to consider the evidence and determine on the evidence and balance of probabilities whether to (i) find the allegation not capable of substantiation and/or (ii) determine whether to initiate disciplinary or other action.

The investigation report is completed by an Ethics Consultant and approved by the Executive Director, ESU. A memorandum is prepared to briefly outline the information contained in the investigation report. The memorandum accompanies the investigation report, which is referred to the decision maker to make a determination on the allegations; and provides for the decision-maker to record their decision in a clear manner.

## **Disciplinary process**

If an allegation is found to be capable of substantiation and the decision maker determines that the alleged conduct warrants the commencement of a disciplinary process, the ESU is responsible for the management of this process. Crown Law undertake the preparation of all required disciplinary correspondence for these matters, in accordance with the Public Service Commission Discipline Guideline.

The ESU is responsible for facilitating the delivery of all disciplinary correspondence to the subject officers. Additionally, the ESU is responsible for providing the Human Resources Branch a copy of the disciplinary correspondence for their file and to update Payroll records, if required.

The Departmental contact point for staff members subject to a disciplinary process is an Officer of the Human Resources Branch.

## **Appeals**

Staff members subject to disciplinary action have the right to appeal the decision made by the decision maker to the appropriate body. This may also include seeking external review or applications for reinstatement.

The ESU is responsible for liaising with the Human Resources Branch and Crown Law in the management of any appeals process.

## **File completion**

Once a file has been completed, the following is to occur by the Ethics Consultant:

1. Written notification to all relevant parties, as required;
2. Ensure local management is aware of the completion and outcome in general terms of the matter;
3. Ensure all documentation (emails, file notes, interview recordings/transcripts, written correspondence, CCTV footage, investigation report and memorandums) relevant to the investigation are saved electronically on the investigation file; and
4. Refer the file to the Administration staff with instructions to close the file.

The Administration staff will complete the following in order to close the file:

1. Updating of ESU registers;
2. Collation of paper file;
3. Completion of run sheet;
4. Burning of the folder to disc;
5. Closing of the file; and
6. Archiving of the file, when required.

## **Record keeping**

All documentation (emails, file notes, interview recordings/transcripts, written correspondence, CCTV footage, investigation report and memorandums) relevant to the investigation file **must** be saved electronically on the corresponding investigation file in line with ESU approved naming conventions (e.g. 2016-02-16 – 1614 – CG email to KT – please deliver report and memo to DDG).

Where there are preserved multiple versions of a documents, all versions, in so far as they reflect the approval chain (from initial author to final approved version) are required to be saved to the corresponding investigation file. Draft versions of any documents prior to approval at each stage of the approval chain are not required.

All documentation relating to a complaint must be retained for seven (7) years after the last action in accordance with the Queensland State Archives 'General Retention and Disposal Schedule for Administrative Records'.

### **Responsibilities for this policy**

The ESU is responsible for the preparation, review and maintenance of the policy. This policy will be reviewed three (3) years from date of approval.

### **Version History**

<b>Version</b>	<b>Revision Date</b>	<b>Revision</b>	<b>Approved By</b>
1.0	February 2016	Creation	Executive Director, Ethical Standards Unit
2.0	May 2019	Revision	A/Executive Director, Ethical Standards Unit

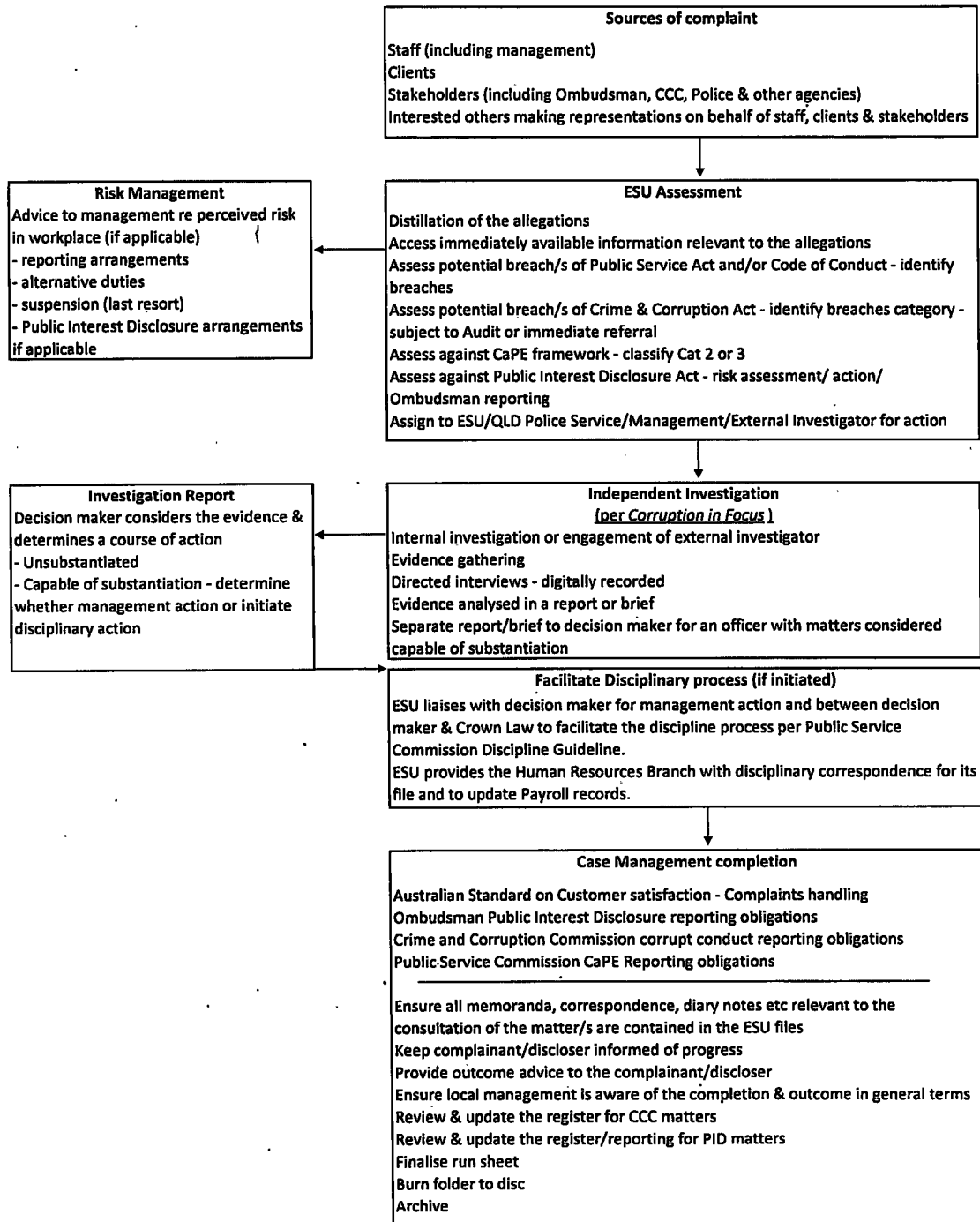
## DJAG Corrupt Conduct & Misconduct Case Management Flowchart


"The Executive Director, Ethical Standards Unit, is involved in the development and delivery of programs to improve ethical culture and ethical decision making across DJAG; manages the investigation of allegations of misconduct and corrupt conduct and the submission of reports and advice to decision makers involving serious workplace conduct and disciplinary issues.

*Allegations of misconduct and corrupt conduct are to be referred to the Executive Director immediately.*

*The Executive Director is also the Crime and Corruption Commission Liaison Officer and Public Interest Disclosure Officer."*

DJAG Intranet



<input checked="" type="checkbox"/> Approved	<input type="checkbox"/> Not Approved
Signed: 	
David Mackle Director-General Department of Justice and Attorney-General	
Date: 20.5.19	



## The 23 protected human rights

<b>RIGHT TO RECOGNITION AND EQUALITY BEFORE THE LAW</b>  SECTION 15	<b>RIGHT TO LIFE</b>  SECTION 16	<b>PROTECTION FROM TORTURE AND CRUEL, INHUMAN OR DEGRADING TREATMENT</b>  SECTION 17	<b>FREEDOM FROM FORCED WORK</b>  SECTION 18
<b>FREEDOM OF MOVEMENT</b>  SECTION 19	<b>FREEDOM OF THOUGHT, CONSCIENCE, RELIGION AND BELIEF</b>  SECTION 20	<b>FREEDOM OF EXPRESSION</b>  SECTION 21	<b>PEACEFUL ASSEMBLY AND FREEDOM OF ASSOCIATION</b>  SECTION 22
<b>TAKING PART IN PUBLIC LIFE</b>  SECTION 23	<b>PROPERTY RIGHTS</b>  SECTION 24	<b>PRIVACY AND REPUTATION</b>  SECTION 25	<b>PROTECTION OF FAMILIES AND CHILDREN</b>  SECTION 26
<b>CULTURAL RIGHTS – GENERALLY</b>  SECTION 27	<b>CULTURAL RIGHTS – ABORIGINAL PEOPLES AND TORRES STRAIT ISLANDER PEOPLES</b>  SECTION 28	<b>RIGHT TO LIBERTY AND SECURITY OF PERSON</b>  SECTION 29	<b>HUMANE TREATMENT WHEN DEPRIVED OF LIBERTY</b>  SECTION 30
<b>FAIR HEARING</b>  SECTION 31	<b>RIGHTS IN CRIMINAL PROCEEDINGS</b>  SECTION 32	<b>CHILDREN IN THE CRIMINAL PROCESS</b>  SECTION 33	<b>RIGHT NOT TO BE TRIED OR PUNISHED MORE THAN ONCE</b>  SECTION 34
<b>RETROSPECTIVE CRIMINAL LAWS</b>  SECTION 35	<b>RIGHT TO EDUCATION</b>  SECTION 36	<b>RIGHT TO HEALTH SERVICES</b>  SECTION 37	