Information Communication and Technology (ICT)

Version Number
1.1

Implementation Date
25/02/2015

Scope
Department-wide, excluding TAFE

Purpose
This procedure provides employees with the requirements to protect, secure and support the department's ICT facilities, devices, services and systems. It also outlines expected behaviours and consequences when using these government resources.

This procedure further enables the provision of a safe and secure ICT environment that supports a personalised and collaborative digital experience.

Overview
This procedure has been divided into the following sections:

1. Use of ICT facilities and devices
2. Departmental mobile devices and their services
3. Bring your own (BYO) personal mobile device
4. Management of ICT business systems
5. ICT security
6. Reporting ICT security incidents
7. Malware and malicious code prevention
8. Identity (ID) and access management
9. Software licence management
10. Backup procedures
11. Metadata schemes
12. Internet
13. Non-departmental ICT service providers

Responsibilities
Assistant Director-General, Information and Technologies:

- nominates the department's single point of contact (Director, Web Services) for registrations with the Queensland Government domain provider.

Director, Platform Operations, Information and Technologies Branch and Corporate Procurement Branch:

- corporately manages and tracks the 'managed print service' facility (office printing on any printing device).
Process

1. Use of ICT facilities and devices

All **employees** have responsibilities and obligations when using the department's ICT facilities and devices which includes access to systems, networks and services such as internet, phone, email, printer, Wi-Fi etc. The department monitors and records use of its ICT facilities including the internet, intranet and email. The department's email system is not an authorised recordkeeping system.

**Employees** when using the department’s ICT facilities and devices must:

- follow acceptable use procedures of the ICT business systems they use
- not use other email systems (e.g. free webmail services) for the distribution of all work related information as privacy, confidentiality and security may be breached
- ensure their use of the internet and email is able to survive public scrutiny and/or disclosure (see the **Use of ICT Facilities and Devices Guideline**)
- transfer emails that form records into an authorised recordkeeping system
- optimise cost associated with printing by minimising their printing requirements, where possible, and ensuring print settings at a minimum are configured as a default to monochrome, double sided and with the toner set to draft quality
- refrain from connecting to colour printers/multifunctional devices assigned for specialised printing (e.g. publications, annual reports etc.)
- report any incident such as receiving anything hateful, offensive or illegal as per Section 6 - **Reporting ICT security incidents** as any wrongdoing may be traced.

**Directors, principals and above:**

- manage and monitor costs, and appropriate use of the departments ICT facilities and devices
- authorises the use of printer/multi-functional devices for specialised colour printing (e.g. annual reports, publications etc.) and actively managing printing to ensure that colour printing is minimised in their business unit or school.

**Teachers and principals will:**

- exercise a duty of care regarding student access to and use of the school's ICT facilities
- provide guidance for use of their ICT facilities and devices within the classroom, including ensuring students understand and follow the school's policies and guidelines. See also the **Advice for State Schools on Acceptable Use of ICT Facilities and Devices**.

**Principals** are to:

- ensure their school develops a policy on acceptable use of the department's ICT facilities and devices (see the **supporting advice**) and that it is understood and acknowledged by school students and parents/guardians at least once every year, either on enrolment or through annual communication with parents/guardians at start of each school year
- implement risk management measures to reduce likelihood of network access to harmful information including monitoring/auditing internet and email activities.

**School web filtering**

**Web filtering** is managed in schools with any accidental access to inappropriate internet sites or where access to a site leads to inappropriate content is reported by the teacher to their supervisor.

The following actions must be taken by the **principal or their delegate** to remove and report the uploading of inappropriate images/footage, to websites, particularly where employees and students are involved or if the school is in some way implicated.
Step 1: Investigate the incident reviewing the web content to determine actions to be taken. If the website is blocked contact the Service Centre by phone on 1800 680 445 to discuss options available or escalate to the Cybersafety and Reputation Management Team for further investigation.

Step 2: If upon investigation, it is immediately apparent that the content threatens or puts in danger students or any community members the principal follows the school’s emergency response process or report the incident to the regional director.

Step 3: Immediately request the student/s to remove content from the website in question, where possible. Alternatively, coordinate the removal with those directly involved or the website’s service provider. Refer to Cyberv bullying and reputation management – Incident management guidelines for principals or contact the Cybersafety and Reputation Management Team on (07) 3034 5035, Cybersafety.ReputationManagement@dete.qld.gov.au or the Regional Technology Manager.

Step 4: Where necessary take action to minimise access to the offensive content by contacting their Managed Internet Service (MIS) administrator to immediately 'block' the website at the school level or the Service Centre by phone on 1800 680 445 to seek departmental 'blocking' of the website.

Step 5: Report any incident involving an employee to the Ethical Standards Unit. See the Advice for State Schools on Acceptable Use of ICT Facilities and Devices for guidance.

Print services

Directors, principals and above must coordinate and manage their business units or schools' print services including:

- using the department's 'managed print service', where possible and where it represents best value for money
- ensuring print services have been optimised to minimise costs
- managing print services billing accounts and costs for printer usage/maintenance
- tracking and monitoring print volume and services with costings where the service is not the department’s 'managed print service'
- tracking and monitoring print services for asset control and audit purposes
- consolidating the purchase of printing services except where centralised purchasing would not be cost effective, such as in remote locations.

The Director, Platform Operations, Information and Technologies Branch together with the Corporate Procurement Branch have been assigned responsibilities for the management and provision of the 'managed print service' facility which includes:

- tracking and monitoring print volume and services with costings
- managing print services through monthly billing accounts which includes cost centre allocations and costs for printer usage/maintenance.

Inappropriate use

Using departmental ICT facilities and devices to engage in inappropriate use is unacceptable. Violating departmental policies may result in restricted access to ICT facilities, departmental disciplinary action (including dismissal) and/or action by the police. The State Government’s position, described in the Cabinet endorsed Use of Internet and Electronic Mail Policy and Principles Statement 2007 is that:
• employees found to be intentionally accessing, downloading, storing or distributing pornography using government-owned ICT facilities and devices will be dismissed
• employees may be disciplined or dismissed for the misuse of the internet or email in respect of material that is offensive or unlawful
• a pattern of behaviour (for example, repeated use) is a factor in determining disciplinary measures (including dismissal).

Some actions by an employee may constitute a crime, under the **Criminal Code Act 1899** or be viewed as serious misconduct (see **Code of Conduct**), and could lead to suspension, exclusion, loss of employment or prosecution. Further information and examples on appropriate and inappropriate use is provided within the Queensland Government's **Authorised and Unauthorised Use of ICT Facilities and Devices Guideline**.

---

**Personal use**

Personal correspondence (emails, text messages etc.) created or passed through the department's ICT facilities and devices can be subject to access requests under Right to Information Act 2009 and Information Privacy Act 2009 (see the **Information Management (IM) procedure's** information release, access and use section).

The H: drive or equivalent, where available, is provided for the storage of personal ephemeral and reference information only.

Limited personal use of departmental ICT facilities, ICT devices and ICT services is acceptable by employees however it can be revoked at any time. It is subject to the same monitoring practices as employment related use and may be subject to disclosure under the **Right to Information Act 2009**.

**Limited personal use** is acceptable by an **employee** provided that such use:

- is infrequent and brief
- does not interfere with the operation of government
- does not violate any state/agency policy (e.g. Queensland Government's **Code of Conduct for the Queensland Public Service**) or related state/commonwealth legislation and regulation
- incurs only a negligible additional expense, if any, to the department
- does not impede that employee's or any other employees' ability to do their jobs
- occurs during off-duty hours (off-duty hours are the periods of time when an employee is not expected to be working, such as during a lunch break or before and after scheduled work hours), whenever possible
- is not for the purpose of generating income for the employee or another individual (i.e. private business, personal gain or profit).

Further details on acceptable and unacceptable behaviours or actions and their consequences see the **Use of ICT Facilities and Devices Guideline**.

---

**2. Departmental mobile devices and their services**

Departmental funded mobile devices, voice, email and data access are provided to employees for officially approved departmental business with **limited personal use**. A **Mobile Devices and Services - Conditions of Use** is provided to each employee on the provision of a departmental mobile device and related services. Costs are charged to the department's corporate accounts.

The provision of a mobile device and their services is provided to **employees** subject to:
The approval for purchase being provided by their director, principal or above based on the requirements of their role to conduct work-related business and is purchased only through Service Centre Online.

Usage complying with:
- this procedure's Section 1 - Use of ICT facilities and devices on acceptable use
- the Queensland Government's Code of Conduct for the Queensland Public Service and the department's Standard of Practice.

Explaining any use, and if required to reimburse expenses that occur.

If required to travel overseas, an approval for work-related business use is approved by their director, principal or higher. An International Roaming Data Plan must be purchased (through Service Centre Online) which will disable the original plan whilst travelling. An allowance of three weeks prior to departure is required to establish the plan.

Supervisors, managers, directors, principals or above must:

- ensure all mobile devices (model/serial numbers) are recorded in an assets register according to Equipment Management for Business Units procedure or Equipment Management for Schools procedure
- ensure the mobile device's unique IMEI (International Mobile Equipment Identity) number is recorded at the time of purchase to facilitate identification should the device be lost or stolen
- when a funded mobile device and its service is used by a number of persons, a local register of individual assignments is maintained for security and reporting reasons
- validate monthly mobile call costs against cost centres for their business units or schools through Infoview
- ensure the recovery of any mobile device and SIM card allocated to an employee who is leaving the department or moving to another agency to avoid liability for costs
- monitor use according to this procedure.

3. Bring your own (BYO) personal mobile device

The department allows access to its ICT systems and networks by employee's personal mobile devices subject to certain conditions. Where available, employees are to consider the use of ICT facilities and devices provided or made available for use by the department.

Employees using personal mobile devices to access the department's network including school networks must:

- seek written approval from their manager, director or principal to connect the personal mobile device
- ensure they meet the department's security requirements (see iSecurity intranet site for details) at a minimum installing, running and updating anti-virus software
- follow departmental procedures, school policies (if applicable), rules on their use and any warnings provided
- accept responsibility for the availability, integrity and confidentiality of departmental information in their care
- operate the mobile device only in areas where the security of the information can be assured. For example, protect information in a public area where other persons may be able to view your information
- use secure passwords (see the iSecurity intranet site for assistance) and lock the device when not in use
- ensure the device is used in a lawful, responsible and ethical manner
- manage stored departmental information in accordance with the level of sensitivity (i.e. information security classification) of that information
- regularly backup departmental information stored on these devices to the department's
network or an authorised recordkeeping system
• after performing a backup remove from the hard drive all departmental files (e.g. information, software and applications) from these devices (e.g. computer, laptop, tablet) when:
  ◦ it is no longer required for departmental work purposes
  ◦ on leaving the employment of the department
  ◦ before any exchange of equipment under warranty or for repair, or
  ◦ before disposal of the device
• ensure all software and other material on the device complies with licencing, copyright and any other intellectual property requirements
• understand that their supervisor, manager, director, principal or above may restrict or deny access to the department's network by any personal mobile device used on departmental premises (e.g. school, central office)
• understand that the department may conduct security audits, assessments and scans of any personal mobile device connected or proposing to connect to the department's network if at any time the security of the network is at risk.

The department does not accept liability for any loss or damage suffered to personally owned devices as a result of using the department's ICT facilities, systems, network or services and is not responsible for any repairs or maintenance. The department further does not provide any technical or software support to an employee's personally owned device.

BYO personal mobile devices within schools
The department allows the use of BYO devices subject to school employees following the requirements above.

A principal may approve student use of personal mobile devices to access the school/department's network. This access to the network is to be provided only if the device meets security requirements (see iSecurity intranet site for details). Schools approving student access to the school/department's network are also required to develop appropriate programs, policies and procedures see Advice for State Schools on Acceptable Use of Departmental ICT Facilities and Devices.

4. Management of ICT business systems

Business system owners and/or information custodians when implementing or updating an ICT business system must:

• implement business rules to safeguard privacy, confidentiality, security and other legislative obligations
• implement appropriate security to protect the ICT business systems from unauthorised access, use, disclosure, corruption or destruction in accordance with Section 8 - Identity (ID) and access management
• review and assess the ICT business system on a regular basis to ensure it continues to satisfy business requirements and its integrity is being maintained through the department's Enterprise Architecture Repository
• classify information assets within the ICT business systems according to requirements within the Information Management (IM) procedure including its information security classification/s
• identify and/or implement service level agreements and information sharing requirements when engaging an ICT service provider (see Non-departmental ICT service providers)
• apply and/or maintain metadata schemes
• establish processes and controls for backup procedures.

The information owner has authority and accountability for the ICT business system.
Decommissioning ICT assets and devices

**Supervisors, managers, directors, principals or above** are to ensure all ICT assets and devices (e.g. computers, photocopiers or any devices) are retired and disposed of in accordance with the [Equipment Management for Business Units procedure](#) and [Equipment Management for Schools procedure](#). Prior to disposal all departmental data/files must be removed to the network or an authorised recordkeeping system. Assistance for this can be provided by:

- in a school contact your [regional technology manager](#)
- [Service Centre Online](#) or Service Centre on 1800 680 445.

5. ICT security

The department has developed, documented, implemented, maintains and continually reviews appropriate security controls and processes to comply with Queensland Government's policy, leading ICT security practices, reporting and auditing requirements, and legislative obligations.

**Employees** must protect and secure the department's information and ICT business systems by:

- ensuring that the ICT business systems they use or that are under their control are operated in a secure manner in accordance with this procedure
- accepting responsibility for the availability, integrity and confidentiality of information in their care
- ensuring that any departmental information they create, handle and store is protected from unauthorised access or amendment where the information security classification is X-in-confidence, protected or highly protected (see the [Information Security Classification and Handling Guideline](#) for further details)
- maintaining a clear desk and screen by protecting X-in-confidence, protected and highly protected information from unauthorised access. This includes physically locking away the information or locking the ICT device when unattended.

The [Information Security Guideline](#) and iSecurity intranet site supports this procedure by providing employees with guidance on ICT security compliance.

**Supervisors, managers, directors, principals or above** must:

- establish business unit or school security control processes including roles and responsibilities for handling and managing of any X-in-confidence and above information, and incorporate these into position descriptions
- provide appropriate induction and on-going ICT security training for users such as [Keys to managing information](#)'s (mandatory) information security course and iSecurity intranet site
- ensure that an annual internal review of ICT security practices, including a risk assessment, is undertaken.

**Operational Security Team, Information and Technologies Branch** provides departmental support and controls for ICT security across departmental ICT business systems and assets, and are responsible for:

- implementing and maintaining appropriate protection of the ICT network's underpinning and ancillary services from internal and external threats (e.g. mail gateways, domain name resolution, time, reverse proxies, remote access and web servers)
- ensuring system change and release management processes include confirmation that appropriate security controls have been applied and the capacity requirements of the system have been considered
• establishing processes to periodically review and test firewall rules and associated network architectures to ensure the expected level of network perimeter security is maintained
• establishing processes to periodically review and update current network security design, configuration, vulnerability and integrity checking to ensure network level security controls are appropriate, effective and up-to-date
• developing security controls to manage all aspects of online and internet activities including anonymity/privacy, data confidentiality, use of cookies, applications/plug-ins, practices for downloading executable code, web server security configuration, auditing, access, encryption
• complying with the department's network security policy and network security control definitions for information exchange (internally or externally)
• periodically performing penetration testing for all critical online services
• establishing security controls for ICT business systems, network infrastructure and applications in line with the Information Management (IM) procedure
• addressing security requirements in all stages of new ICT systems, network infrastructure and applications
• establishing security controls during all stages of system development, as well as when new systems are implemented and maintained in the operational environment
• ensuring appropriate change control, acceptance and system testing, planning and migration control measures are being adhered to when upgrading or installing software in the operational environment
• ensuring accurate system security records to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation
• establishing processes (including data validity checks, audit trails and activity logging) in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure
• developing and implementing processes to manage software vulnerability risk for all ICT business systems, network infrastructure and applications
• implementing a patch management program for operating systems, firmware and applications of all ICT assets to maintain vendor support, increase stability and reduce the likelihood of threats being exploited
• creating and managing Secure Socket Layer (SSL) Certificates.

Platform Operations, Information and Technologies Branch will:

• regularly monitor the system's capacity to ensure the risks of system overload or failure which could lead to a security breach are avoided
• synchronise all ICT assets to a trusted time source that is visible and common to all
• develop, maintain and test business continuity and ICT disaster recovery plans and processes for ICT business systems under their control in accordance with the department's Business Continuity Management (BCM) procedure.

6. Reporting ICT security incidents

Employees must report any ICT security incident to their supervisor, manager, principal or above (as appropriate) who will follow the steps below:

Step 1: Resolve the incident locally, if possible.
Step 2: If the incident cannot be resolved locally, submit an information security incident report or contact the following (as appropriate):

• for technology issues contact Service Centre on 1800 680 445 or Service Centre Online
• Ethical Standards for violations of the Queensland Government's Code of Conduct for the
7. Malware and malicious code prevention
The department installs anti-virus software to prevent, detect, remove and report computer virus and malware attacks or malicious code. A range of control measures have been implemented to protect business units and schools. In addition to this all users must:

- ensure they do not disable or interfere with the operation of antivirus software
- ensure departmental purchased ICT devices such as laptops, tablets etc. approved for work use are at least weekly connected to the network for antivirus software updates
- exercise caution when opening email and related attachments that they do not expect
- not download software from the internet unless authorised by their manager, teacher or above. If appropriate, scan downloaded software for malware and malicious code. For technical assistance, contact the Service Centre Online
- not develop, distribute or run any computer programs or code that is intended to replicate itself, cause damage, and/or impede the performance of any computer, software application or network whether malicious or otherwise
- scan all files and information contained on mobile media and storage devices for malware and malicious code prior to being used on any department ICT device. Scanning can be either manual or automated
- where possible, isolate infected devices by either turning it off or disconnecting the network cable
- report any malware and/or malicious code attacks to their supervisor as per Section 6 - Reporting ICT security incidents.

System security administrators with ICT security responsibilities within the department must:

- manage and coordinate activities and resources to prevent, detect, remove, report and respond to incidents of malware and malicious code
- establish and implement a mandatory procedure on scanning to ensure that traffic entering and leaving the department’s network is appropriately scanned for malicious or unauthorised content
- define and conduct vulnerability/integrity scans of core software to ensure detection of unauthorised changes
- ensure departmentally approved antivirus software has been installed on all specified corporate and school ICT devices, are configured to the department's installation guide available on OnePortal (DET employees only), and are regularly updated with new definition files
- ensure where school computers are managed by an ICT service provider, that the service level agreement contains a provision whereby antivirus software is installed and regularly updated on computers.

Breach of security
All users accessing departmental computers, tablets, laptops, smart phones via the departmental networks who breach and/or bypass the information security malware and malicious code prevention measures may be subject to disciplinary action. Such conduct may result in restriction and/or suspension of access privileges. Where users within the community have been identified as breaching and/or bypassing the information security malware and malicious code prevention measures, access rights will be withdrawn.

Depending on the severity of the user's conduct, the matter may be reported to state or federal...
police. This applies to employees, students and users in the community. The department monitors and audits the antivirus software and records any or all malware and malicious code related activity. Users may be called upon to explain any incident.

8. Identity (ID) and access management
The department controls access to its ICT business systems and information assets based on their information security classification, authentication processes, legal/legislative obligations, business requirements and assessed/accepted risk. User identity (ID) accounts for generic, employee and non-departmental users are managed through the iRegister system.

Access to any ICT business system is determined by an employee's supervisor, manager, director, principal or above based on the requirements of the job role and the information security classification/s of the system/content. This access will be disabled or modified when their requirements change, such as a change in job role within the department, if a person leaves the department permanently, or is on leave for a prolonged period.

Employees and non-departmental users must:

• acknowledge or take appropriate action on receiving warnings, when accessing or while using the department's ICT business systems
• ensure passwords are hard to guess and kept secure/secret (see the iSecurity intranet site for assistance)
• where work identification and location details are provided within a directory such as a phone directory that these details are kept up-to-date.

Managers, directors, principals and above who control access to information within a specified application or ICT business system must:

• ensure the processes within this procedure and Identity (ID) and Access Management Guideline are adhered to
• ensure that where personal statements are used such as in a directory, personal work particulars are verified
• ensure that all forms used to collect information from users include a privacy statement including user access application forms
• ensure that a user's access is cancelled when the user has resigned or been seconded, dismissed or suspended. Or for schools, where a student has left, had their enrolment cancelled, been suspended or excluded, the Managed Internet Service (MIS) system is used to deactivate the student. If an account is to remain active the accountable officer is responsible for the actions that occurs within this account
• determine the need for continuation of an employee's account, for example where the role of an employee changes. Consideration for deactivation of an account should include job tenure (permanent or temporary), inter-agency transfer, extended leave and resignation
• manage identities such as continuation or deactivation of an account
• advise system administrators through approved change management procedures when employees commence duty, change their name and/or personal details, or leave the department
• inform business system owners and/or information custodians through approved procedures when employees should be deactivated for unacceptable use of ICT business systems
• regularly educate employees and students on adherence to password and security requirements of the ICT business system in use
• ensure that information about identities under protection orders is classified as highly protected and access is restricted in accordance with Information Management (IM)
procedure's information security classification section

- if within a school, determine the need to deactivate a student's account during vacation periods. A risk assessment should consider a student's education/training outcomes. Where accounts are to remain active (e.g. to access notices) following a student's completion of all course requirements, the risk assessment should consider the need and circumstances for access against network protection.

---

**Business system owners** and/or **information custodians** accountable for a specified application or ICT business system must:

- determine the application or ICT business system's information security classification/s in accordance with **Information Management (IM)** procedure's information security classification section
- regularly review and identify users, their roles, registration identification requirements and level of information access in accordance with the **Identity (ID) and Access Management Guideline**.

**Note:** The location of a user while accessing ICT business systems e.g. employees accessing a business system from desks in central office or district office, may require a lower level of authentication than the same employee accessing the same system from home or while mobile
- conduct a risk assessment on the consequences of unauthorised access to information within the ICT business system
- approve the use of generic accounts based on a documented business case which includes a risk assessment, benefits, costs and alternative options. The use of generic account/s should be kept to a minimum with strict and proper procedures for use
- ensure the user access application forms include a privacy collection statement that indicates how personal information collected will be used and protected. See the **Personal Information Guideline** for guidance information on privacy statements
- protect the identities of users, including students enrolled in schools who have become subject to legal orders, including but not limited to child protection orders, such that only authorised employees (e.g. principal or delegate) have access.

---

**System administrators** who are responsible for the technical aspects of providing access to a specified application, ICT business system or network on behalf of the business system owner and/or the **information custodian** must:

- ensure appropriate security mechanisms are in place to protect data from unauthorised access or modification and, accidental loss or corruption
- identify and implement access restrictions and segregation/isolation of systems into all infrastructures, business and user developed applications
- manage directories of users including allocating and resetting passwords, user access, security and data backup, and storage of directories
- establish controls and processes for user registration, authentication management, access rights and privileges are in accordance with **Identity (ID) and Access Management Guideline** and in the case of schools match student enrolments
- manage changes to access rights whenever a user's role changes or the protection of a user is required in accordance with the **Identity (ID) and Access Management Guideline**
- implement audit logging with relevant internal controls, monitoring, reviewing and processing mechanisms commensurate with the information security classification level.

---

9. **Software licence management**
The department implements and manages the purchase, installation, maintenance and retirement
of software and their licences. To ensure compliance employees must:

• comply with the software’s terms and conditions of use
• not breach any copyright or piracy laws
• acquire, where possible, all software for departmental ICT devices through Service Centre Online (a list is available under ’Request’ > ’Software & business systems’)
• not copy any unauthorised software (including any personally owned software) to their departmental ICT device
• notify a supervisor, manager or above if they become aware of unlicensed or unauthorised software
• ensure discounted software purchased through the department for home use complies with its conditions of use including uninstalling the software when leaving the department or deleting the software when their ICT device is sold or disposed of
• ensure personal mobile devices connected to the department’s network have appropriate licences for the software being used
• direct any software licence enquiries such as compliance and eligibility through the Service Centre.

Managers, teachers, directors, principals and above must:

• ensure that a software asset register is maintained within their business unit or school which details all software purchases (regardless of method of purchase/acquisition) including ownership, allocation, site licences and any variations approved by the licence owner but excluding any licence distributed as part of the department’s managed operating environment (MOE) (DET employees only)
• coordinate their business unit or school purchases of software applications in compliance with the Purchasing and Procurement procedure through a Government Information Technology Contracting (GITC) Framework accredited supplier
• ensure that software licences, under their control, are procured under the name of ‘The State of Queensland acting through the Department of Education and Training
• where they have directly purchased software, take full responsibility for the management of the software, its updates, its licence, its fees and terms and conditions of use
• manage the retirement or replacement of any off-the-shelf software with a high or medium business impact before it reaches the end of mainstream support by the vendor unless the Director-General has formally accepted the risk of not doing so
• coordinate the de-installation of software identified as unlicensed, inappropriate, or deemed as an unsupported application through Service Centre Online
• acquire any open source software (OSS) in accordance with GITC framework and that use, modification and distribution adheres to the OSS licence conditions
• not use open source software where software applications have been mandated for whole-of-government use e.g. SAP Financial Management
• contribute or release any departmental open source software subject to a business assessment including legal reasons and appropriate copyright licence
• undertake an annual review of software compliance in their business unit or school which excludes licences distributed under the MOE
• ensure school managed BYOD programs comply with software licensing conditions for non-departmental owned device.

Executive Director, IT Solutions and Operations, Information and Technologies Branch is responsible for processes for the management, maintenance, monitoring, reporting and retirement of enterprise software and their licences providing advice on:

• software management processes to support strategic direction, purchase, installation, configuration, assurance, storage, security, maintenance and retirement of software and
licences
• the implementation of a software asset register/s to monitor, record and manage enterprise
  software use (including the storage of original media and licence documentation)
• compliance with software licensing agreements.

10. Backup procedures
Information and system backup procedures and archiving must be in place to ensure that in the
event of a loss restoration can take place within acceptable parameters to ensure business
continuity.

Employees must not store the only copy of important information on storage media that are
not regularly backed up such as on local hard drives (internal such as C: and D: drives or
external) of computers or USB's. Store important information on a network drive which is
regularly backed up or maintain within an authorised recordkeeping system.

Business system owners and/or information custodians who set and define the rules for a
specified application or ICT business system must establish processes and controls for:
• backing up information including physical and environmental, based on the ICT business
  system’s information security classifications
• implementing backup cycles related to the business risk, frequency with which data and
  software is changed and the criticality of the system to business operations. The cycle
  should include, as a minimum:
  ◦ incremental daily backups of data and full weekly backups of all data, operating system
    and applications
  ◦ backups of the complete operating system and applications on a cycle deemed
    appropriate by the Director, Platform Operations, Information and Technologies
    Branch but as a minimum, on a monthly basis
• maintaining a register of backups including verification of their success
• documenting and making available backup and restoration procedures to employees that
  require it and are available at the backup location
• providing the means to recover the information by storing it at its backup location or making
  it available from an identified source
• using a regular cycle of backup media for all backups, with at least one copy in each
  monthly cycle stored off-site
• the performance of backups before and after major changes to the operating system,
  system software or applications system
• considerations to upgrade to new technologies to ensure that backup data is able to be
  read in the new environment
• implementing a cycle of regular tests to verify that it can be recovered from the backups
  produced
• retaining a cycle of backup media of all information required to meet customer service, legal
  or statutory obligations
• business continuity and disaster recovery:
  ◦ store offsite at least one copy in each backup cycle and restoration procedures
  ◦ undertake regular tests (held at least annually) to ensure that backup procedures meet
    requirements of the department’s business continuity and ICT disaster recovery plans
• the retainment of backups are to be kept only for as long as required for administrative
  purposes except those required to meet evidence of business activity, contractual, legal or
  statutory obligations for archive purposes which must be periodically tested to ensure their
  integrity in line with requirements defined by Queensland State Archives
• backup media to be disposed of in accordance with the Equipment Management for Business
  Units procedure or the Equipment Management for Schools procedure.
11. Metadata schemes

Business system owners and/or information custodians must apply a metadata scheme to their ICT business system including datasets, records, web-based information and web services to ensure ease of search and discovery. Whilst it is not mandatory for schools, schools are encouraged to apply metadata to web pages and authorised recordkeeping systems to enhance information management and resource discovery.

The following metadata schemes are available to be applied to an ICT business system:

- **Australian Government Locator Service (AGLS)** – is preferred for websites and is the minimum required metadata scheme for any ICT business system
- **Queensland Recordkeeping Metadata Standard (QRKMS)** (Queensland State Archives) – is preferred for authorised recordkeeping systems and adherence to all mandatory elements ensures records are complete, accurate, reliable and useable
- **Australia and New Zealand Land Information Council (ANZLIC)** (ANZLIC - the Spatial Information Council) – is preferred for spatial data systems
- **Australian Government Recordkeeping Metadata Standard Version 2.0, July 2008** (National Archives of Australia)
- **ANZ–LOM** (National Digital Learning Resources Network - Education Services Australia)
- **Vetadata - E-standards for Training** (Flexible Learning Advisory Group).

All mandatory elements of a metadata scheme must be included within the ICT business system. When implementing metadata schemes the **business system owner** and/or **information custodian** must:

- apply consistent metadata, where applicable, use mechanisms (such as controlled vocabulary, taxonomy, thesaurus (see below), etc.) and automate the input of known consistent values
- where an extension of the elements (use of optional or conditional elements) for the schemes is required to meet business requirements, the extension must be implemented according to the metadata extension methodology in the scheme being used
- where applicable, ensure the metadata is extractable or exportable in a XML format so that departmental resources are accessible through other search engines and educational websites
- put in place governance controls for the management of the metadata under their custodianship to review its capture, quality, accessibility, currency and accuracy.

The **business system owner** and/or **information custodian** must consider a thesaurus for automation within a metadata scheme which is mandatory within authorised recordkeeping systems:

- **Corporate Thesaurus – Introduction** (DET employees only)
- **Corporate Thesaurus – Terms** (DET employees only)
- **Business Classification Plan** (DET employees only) – quick guide to controlled vocabulary used for classifying, titling and indexing records.

Other thesauruses can be used subject to their applicability to the ICT business system's use and sharing of information:

- **Australian Thesaurus of Educational Descriptors (ATED)** (Australian Council for Educational Research) – definitive reference on Australian terminology in the area of education
- **Schools Online Thesaurus (ScOT)** (Education Services Australia) – a controlled vocabulary of
terms used in Australian and New Zealand schools including educational and administrative processes

- **VOCEDplus subjects and keywords** (National Centre for Vocational Education Research) – an extensive list of educational subjects and keywords
- **Australian Public Affairs Information Service (APAIS)** (National Library of Australia) – humanities and social sciences subject index
- **Dewey Decimal Classification (DDC)** (OCLC) – library classification system.

The **Director, Web Services, Information and Technologies Branch** assists in the implementation of metadata schemes for websites. The **Manager, Information Services, Information and Technologies Branch** will advise on all other metadata applications in particular recordkeeping.

**12. Internet**

All internet websites managed by **employees** must provide for accessibility and usability requirements consistent with Queensland Government standards and branding guidelines. When providing an online presence **employees** who develop or manage departmental websites must:

- ensure the website is managed to ensure timely reviews, appropriate metadata and recordkeeping processes
- ensure the site complies with the Queensland Government's **Consistent User Experience Standard** (CUE) and Corporate Identity (see the department's **Communication and Marketing Guide** (DET employees only)), and the required compliance levels of the **World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG)**
- contain contact information, privacy notices, provisions for customer feedback and information requests, disclaimer notices, and the **Australian Governments Open Access and Licensing Framework (AusGOAL)** creative commons licences.

All websites must be hosted within web hosting services authorised by the **Executive Director, Web and Digital Delivery**. This includes all websites for school activities including websites that an employee creates to support classroom activities.

School websites have a partial exemption from CUE and advice on this can be obtained from **Web Services, Information and Technologies Branch**. For more information see OnePortal's Website development and support web page or your **Regional Technology Manager**.

**Domain names**

**Employees** must ensure they use qld.gov.au or eq.edu.au for domain names and not use non-government domain names unless there is a compelling reason to do so and permission is received in accordance with this procedure.

**Employees** who require a new, change, decommission, deregistration, exemptions etc. for a domain name, sub domain name or fifth level domain and/or web hosting services must log a request through **Service Centre Online**. The request will be forwarded to **Web Services** who will provide advice, assistance and ensure the correct approval process is undertaken.

If the deregistration of the domain name is a result of closure of an educational institution, **Web Services** will advise and assist the school or regional office and the **Manager, Information Services** in the decommissioning of the website in accordance with **Information Management (IM)** procedure recordkeeping section.

Domain names are to be promoted in advertising according to **Your Guide to Queensland Government Advertising**.

Domain names are paid for by business units. Schools are not required to pay for their primary
domain (e.g. eq.edu.au) but additional domains will incur a cost. **Director, Web Services** must approve all new domain names.

Exemptions from domain name and web hosting requirements under this procedure is sought by an employee preparing a business case, in the form of a general briefing note, and submitting this for approval to the **Assistant Director-General, Information and Technologies**.

**Principals’** accountability for websites extends to websites established for school groups and activities such as Parent & Citizens' Association (P&C) or other form of school council.

The **Director, Web Services** is the nominated delegate as the single point of contact within the department for registrations with the Queensland Government domain provider and is responsible for approving and registering all domain names including fifth level .gov.au sub-domains (e.g. project.dete.qld.gov.au). The role is also responsible for maintaining the department's central register of domain names with their renewal dates, registration details and passwords.

### 13. Non-departmental ICT service providers

The department supports the provision of non-departmental ICT service providers for the storage and processing of data including cloud and offshore computing services to drive better performance in the department's ICT service delivery to the community and within government.

The ICT service will usually be a type of managed service which is when, either (a) the provider agrees under a contractual arrangement/agreement to deliver ICT services to meet all, or part of the ICT requirements of the business unit or school, or (b) the provider manages the external delivery of ICT based services to students/parents/employees on behalf of the business unit or school. Examples of ICT services include, but are not limited to:

- online administrative and communication tools e.g. Short Message Service (SMS) products, interview scheduling, identification 'smart' cards, conference registration, phone applications, consultation and survey tools
- online electronic document printing services specialising in printing and binding of reports/year books/newsletters/student work/calendars etc.
- online self-paced services for curriculum related purposes such as testing and recording students' achievement or similar
- online document scanning, electronic document management and data storage services.

**Employees** must consider and determine the information security classification of the information to be used or created when considering the procurement or use of ICT services. Information with an information security classification of highly protected **must not** be stored or transmitted offshore.

### Process

The non-departmental ICT service provider **flowchart** provides an overview of the process for **employees** to consider when purchasing or using an ICT service (whether for a fee or not) from a source other than the department.

**Step 1 – ICT service availability:** Determine the type of managed service needed, the information and/or data to be collected or used, and the information security classification of the information and/or data.

Where available use a departmental secure ICT service e.g. for corporate and schools through the [Learning Place](#), [OnePortal](#), [OneSchool](#), [Managed Internet Service (MIS)](#) or the department’s or school’s internet website. **Employees** must log a request for ICT services through [Service](#).
Centre Online who will forward the request to the appropriate business unit to confirm if an ICT service is currently available.

Where a departmental ICT service is not available the employee must seek approval to proceed from a director, principal or above to continue to the next step.

**Step 2 – Review service providers**: Determine if there is an ICT service provider with a Government Information Technology Contracting Framework (GITC) accreditation that will address your business unit or school's requirement. If there is a suitable GITC accredited supplier or an ICT service provider that will seek GITC accreditation then continue to next step.

If an ICT service provider is not available with GITC accreditation nor be willing to seek accreditation, you must seek the assistance of the Corporate Procurement Branch to review the proposed ICT service provider's terms and conditions for suitability based on the service requirements and its information security classification considering:

- identifying whether the website displays recognised security and privacy standards e.g. Secure Socket Layer (SSL), https or privacy/security seals, if required
- examining the ICT service's privacy policies to understand how it will handle any protected or highly protected information
- examining the ICT service's terms of use to identify how the supplied data/information will be handled. For example, will the information be sold or traded for marketing purposes? How does the site handle intellectual property such as copyright?
- contacting the ICT service provider to ask whether they offer a modified terms of use/privacy agreement for government entities, if required
- checking for tools on the site that allow control of access to the site and the information contained within to be amended, exported and/or deleted
- knowing where the data/information will be stored, that is, in which country the ICT service provider's servers are located
- researching thoroughly the ICT service provider using a search engine or reputable ICT source to identify reports of security or privacy breaches or other issues of concern.

If the ICT service provider's terms and conditions, and privacy controls are not available seek advice from Corporate Procurement Branch and/or do not use the ICT service.

**Step 3 – Risk assessment**: Undertake a risk assessment using a partly populated risk matrix, the Enterprise Risk Management procedure and/or the Queensland Government's ICT risk management tools and techniques. Consider whether the benefits of using the ICT service outweigh the risks involved, particularly if a contract/agreement with the necessary privacy or control clauses is not used and if it has an information security classification of protected or below (e.g. personal information could be transferred overseas) (see Personal Information Guideline).

Data/information stored, processed and/or hosted overseas is acceptable if consideration of the business impact, establishment and ongoing costs, business continuity, risks, issues and mitigation strategies have been undertaken, and it has an information security classification of protected or below. Refer to the Queensland Government's ICT-as-a-service: Decision Framework - Overview (including its risk assessment guidelines), and the department's Cloud Computing Decision Framework (DET employees only) for assistance.

Any data/information stored and/or processed overseas with a security classification of protected or below must be approved by the Director-General or a nominated delegate representing the business of the department this is in addition to any other required approvals.

The following is to also be considered:
• if the contract or other agreement binds the ICT service provider to comply with the *Information Privacy Act 2009* and the requirements in Section 5 - ICT security
• use specific confidentiality clauses in circumstances where the contractor has access to personal information of students, employees or clients
• define the maximum acceptable downtimes for ICT services
• limit information provided to the ICT service provider to that which is necessary for the service to operate efficiently, for example, do not provide full name and address if only an email address is required
• determine any detriment to the individual or corporation if the information is out of date or inaccurate
• provide alternative ways of delivering the ICT service:
  ◦ to people without access to the service. For example, if the parent does not have internet access or does not have the program on their computer
  ◦ in instances of a permanent/temporary 'failure or incapacity to deliver' the ICT service. For example, if the service is SMS text messaging in an emergency, alternative mechanisms should be in place if mobile signal strength is lost or the recipient does not have a mobile phone
• ensure compliance with *Advertising and Sponsorship procedure* if sponsorship from a supplier is being considered or sponsorship is part of the product or services on offer
• costs, if any, must be monitored and where necessary remove, archive or close the ICT services that are not being used
• processes are to be put in place to periodically review the ICT service providers' agreement and update this where necessary to ensure they address any changes in business requirements and remain compliant with the department's policies.

^ Top of page

**Employees** must capture and manage records created in the decision process of the ICT service in accordance with the *Information Management (IM) procedure's recordkeeping section. This includes the risk assessment, details of the information security classification for the information, a list of the types of information managed by the ICT service provider as well as detail about the activity being undertaken.

If the ICT service is to go ahead follow the *Purchasing and Procurement procedure* obtaining advice for protection or privacy clauses as necessary.

**Manager, directors, principals or above** who engage ICT service providers that handle personal information must:

• monitor the service provision to prevent loss, unauthorised access, use, modification, disclosure or any other misuse of personal information
• identify ICT service providers in *privacy notices* where there is an established long-term outsourcing of a particular departmental function. When the ICT service provider changes regularly but outsourcing is ongoing, describe the nature of the services in the *privacy notice* rather than naming the ICT service provider
• when an ICT service provider cannot be bound by contract include an online *privacy notice* in correspondence or on the website to indicate that the ICT service provider will hold a copy of the information and use it in accordance with their terms and conditions
• seek consents from individuals if their personal information is to be used in accordance with *Obtaining and Managing Student and Individual Consent procedure* to use, record or disclose copyright material, image, recording, name or personal information.

^ Top of page

**Principals** will have to determine whether informing and/or seeking parents/guardians, students, Parent & Citizens' Association (P&C), or other form of school council approval or support for such
services is needed outlining:

- the purpose of the service and why it is to be used
- whether personal information will be disclosed to the ICT service provider, or what information the provider is collecting
- how personal information will be used, and whether it will be disclosed and/or transferred out of Australia. The department has no control when such information is transferred overseas, e.g. stored on servers located in another country
- whether the individual is able to unsubscribe from the service and how this is to be done.

**Online Resources**

**Attachments:**

- Use of ICT Facilities and Devices Guideline
- Advice for State Schools on Acceptable Use of ICT Facilities and Devices
- Mobile Devices and Services - Conditions of Use
- Information Security Guideline
- Identity (ID) and Access Management Guideline
- Non-departmental ICT service provider risk matrix
- Non-departmental ICT service provider flowchart

**Supporting documents:**

- Queensland Government Chief Information Office policies and standards
- Government Information Technology Contracting (GITC) Framework
- Public Service Commission policy: Use of Internet and Electronic Mail Policy and Principles Statement
- Queensland Government's Code of Conduct for the Queensland Public Service

**Review Date**

1/05/2015

**Definitions**

**Authorised recordkeeping system**
A system designed to capture, manage and provide access to records through time using a rigorous set of business rules which are intended to preserve the context, authenticity and integrity of the records. Authorisation is provided by a principal or, an executive director or above, ensuring compliance the recordkeeping requirements of the [Information Management procedure](#).

**Business system owner**
Responsible for the maintenance, support and operation of the business system ensuring it is fit for purpose and meets the needs of information owners.

**Employee**
Any permanent, temporary, seconded or contracted staff member, contractors and consultants, volunteers who assist staff with their professional duties, or other person who provides services on a paid or voluntary basis to the department that are required to comply with the department's policies and procedures. Within schools this includes principals, deputy principals, heads of departments, head of curriculums, guidance officers, teachers and other school staff who use information and communication technology.

**ICT asset**
ICT hardware, software, systems and services used in the department’s operations including physical assets used to process, store or transmit information.

**ICT business system**
Information technology systems or applications designed to automate and support the undertaking of a specific business process or processes. They may create, receive, manage and maintain business information relating to business processes.

**ICT devices**
Electronic equipment designed for a particular communication and/or function, including but not limited to computers, mobile devices, television sets, digital or analogue recorders such as DVD and video, facsimile machines, photocopiers and, printers and other imaging equipment.

**ICT facilities**
An electronic service designed for a particular communication and/or function, which includes but is not limited to electronic networks, internet, extranet, email, instant messaging, webmail, fee-based web services and social media.

**ICT facilities and devices**
See definitions for ICT devices and ICT facilities.

**ICT service**
Provision of telecommunications services that carry voice and/or data and includes applications, hosting, storage, and cloud based services etc.

**Information asset**
Is an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling the department to perform its business functions. This includes transactional information in ICT business systems, documents and mail

**Information custodian**
Delegated by the information owner to set and define the rules of an information asset to ensure the information asset is appropriately managed to maintain its currency, integrity and availability. This includes identifying its information security classification/s and, registering and maintaining its details within the department's Information Asset Register.

**Information owner**
The Director-General, Deputy Director-General or Assistant Director-General who approves the rules for the information asset and has authority and accountability for the collection and management of the information asset.

**Mobile device**
Is a type of ICT device and includes mobile and smart phones, laptops, notebooks, tablets, personal digital assistants (PDA), eBook readers, game devices, voice recording devices, cameras, USB drives, flash drives, DVDs/CDs or hard disks, and other electronic storage media or hand held devices that provide retention and mobility of data. A voice only, or voice and data transmission, or data transmission only service may be purchased separately to the device. Data transmission provides internet access for web browsing and email.

**Non-departmental users**
Persons who participate in departmental business processes but are not employees (see definition) for example, parents, medical service providers, work experience supervisors, pre-service teachers, community users and other government employees.

**Personal mobile device**
A mobile device owned wholly by the individual or employee and not by the department, or
whereby the mobile device is being paid for by the individual under an arrangement with the department where at the end of the arrangement the individual will personally own the device.

**School**
Relates to Queensland State Schools including independent public schools. School website Any website setup and/or operated for schools including classroom activities, that may or may not be branded with the school name.

**User**
Any individual or entity accessing the department's ICT business systems and/or applications including employees, students, adults (parents/caregivers), business partners and/or the wider community.

---

**Authority**

- [Queensland Government Chief Information Office policies and standards](#)

**Related Policy Instruments**

- [Criminal Code Act 1899](#)
- [Financial Accountability Act 2009 Section 61, 46L (3)-(4)](#)
- [Financial and Performance Management Standard 2009 Sections 7, 8, 21 and 28, 27 (3)](#)
- [Information Privacy Act 2009 Sch 3 Part 3, Chapter 2, Parts 1, 3 and 4, Part 2 Section 48](#)
- [Right to Information Act 2009 Part 2 Section 28](#)
- [State Procurement Policy](#)
- [Information Communication and Technology (ICT) policy](#)

**Attachments**

- [Advice for State Schools on Acceptable Use of Departmental ICT Facilities and Devices](#)
- [Identity (ID) and Access Management Guideline](#)
- [Information Security Guideline](#)
- [Mobile Devices and Services - Conditions of Use](#)
- [Non-departmental ICT service provider risk matrix](#)
- [Use of ICT Facilities and Devices Guideline](#)
- [Non-departmental ICT service provider flowchart](#)

**Contact**

For ICT support, technology issues, operational security breaches:

- log a job with [Service Centre Online](#), or
- call Service Centre by phone on 1800 680 445

For regional school ICT activities and issues, creating websites and the removal of inappropriate content on internet websites contact your [Regional Technology Manager](#).

For assistance or advice on issues relating to inappropriate online behaviour and content contact:

- Cybersafety and Reputation Management Team, Learning Technologies
  *Phone:* (07) 3034 5035
  *Email:* [Cybersafety.ReputationManagement@dete.qld.gov.au](mailto: Cybersafety.ReputationManagement@dete.qld.gov.au)

For assistance on new, registration, change, decommissioning and recording of domain names, web hosting services contact:
• **Web Services**
• Log a job with [Service Centre Online](#)
• Call Service Centre on 1800 680 445 (press option 3, 3 to go direct to Web Services)
  *Email: [webworkrequest@dete.qld.gov.au](mailto:webworkrequest@dete.qld.gov.au)*

To report allegations of suspected official misconduct:

• Ethical Standards Unit
  *Phone: (07) 3237 0255*
  *Email: [ethicalstandards@dete.qld.gov.au](mailto:ethicalstandards@dete.qld.gov.au)*

For policy advice on this procedure, contact:

• Manager, Information Policy - ICT Governance, Strategy and Policy
  *Phone: (07) 3034 4313*
  *Email: [kylie.gill@dete.qld.gov.au](mailto:kylie.gill@dete.qld.gov.au)*

**Uncontrolled Copy Disclaimer**

*Uncontrolled copy.* Refer to the Department of Education and Training Policy and Procedure Register at [http://ppr.det.qld.gov.au](http://ppr.det.qld.gov.au) to ensure you have the most current version of this document.