Procedure

Use of ICT systems procedure

Version: 1.5 | **Version effective**: 19/12/2024

Audience

Department-wide

Purpose

This procedure outlines the responsibilities and processes for employees to protect, secure and support the department's information and communication technology (ICT) facilities, devices, services and systems. It also outlines expected behaviours and consequences when using these government resources.

Overview

Nil

Responsibilities

All employees have responsibilities and obligations when using the department's ICT facilities and devices.

Owners and/or custodians when implementing or updating an ICT business system are responsible for:

- implementing business rules to safeguard privacy, confidentiality and security obligations including protecting the ICT business system from unauthorised access, use, disclosure, corruption or destruction
- reviewing and assessing the ICT business system on a regular basis to ensure it continues to satisfy business requirements and maintains its integrity. For further information, contact the Enterprise Architecture team on ICT.PandA@qed.qld.gov.au
- classifying information assets within the ICT business systems according to requirements within the Information security procedure
- identifying and/or implementing service level agreements and information sharing requirements when engaging an ICT service provider in accordance with the Non-departmental ICT service providers procedure
- applying and/or maintaining metadata schemes
- establishing processes and controls for backup procedures.

Supervisors, managers, directors, principals or above are responsible for ensuring:

- appropriate use of the department's ICT facilities and devices including costs incurred
- all ICT assets and 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 information on ICT assets or devices are moved to the department's network or an authorised recordkeeping system. Assistance for this can be provided by in a school contact your regional technology manager (DoE employees only) or Services Catalogue Online (DoE employees only).

Employees are responsible for ensuring:

- acceptable use procedures are followed for business systems they use
- ICT systems are not used for the purpose of copyright infringement
- other email systems (e.g. webmail services) are not used for the distribution of work-related information
- individual use of the internet and email is able to survive public scrutiny and/or disclosure (see the Use of ICT facilities and devices guideline)
- emails that form records are saved into an authorised recordkeeping system
- student personal information is not emailed outside the department's network
- their limited personal use of ICT systems and devices 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
- information stored on network drives is regularly backed up or maintained within an authorised recordkeeping system
- the protection of passwords associated with any system or application to which they have access
- printing requirements are minimised, and print settings are configured as a default to monochrome, double sided and with the toner set to draft quality
- colour printers/multifunctional devices assigned for specialised printing (e.g. publications, annual reports etc.) are used only when required
- incidents such as receiving hateful, offensive or illegal material are reported
- unsolicited email 'spam' is reported to Cyber Security (Operational.Security@qed.qld.gov.au).

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 and legal 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

- ensure their school policy includes a 'repeat infringer' clause for copyright infringement e.g. 'Students are prohibited from using the school's ICT network for the purposes of copyright infringement. If you are found to be repeatedly engaging in activities contrary to this policy, your ICT network access privileges may be suspended.'
- implement risk management measures to reduce likelihood of network access to harmful information including monitoring/auditing internet and email activities.

The Director, ICT Infrastructure Services, Information and Technologies Branch and Corporate Procurement Branch is responsible for:

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

Process

Personal use of ICT facilities and devices

Limited personal use of departmental ICT facilities, ICT devices and ICT services is acceptable 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* (Qld).

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

- is infrequent and brief and does not interfere with the operation of government and incurs only a negligible additional expense, if any, to the department
- 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
- 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.

Further details on acceptable and unacceptable behaviours or actions and their consequences see the Use of ICT facilities and devices guideline.

Personal correspondence created or passed through the department's ICT facilities and devices can be subject to access requests under *Right to Information Act 2009* (Qld) and *Information Privacy Act 2009* (Qld).

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

Inappropriate use of ICT facilities and devices

Inappropriate or illegal use of departmental ICT facilities and devices may result in restricted access to ICT facilities, departmental disciplinary action (including dismissal) and/or action by the police. Under the Queensland Government's Use of internet and email policy:

- 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* (Qld) or be viewed as serious misconduct (see Code of Conduct for the Queensland Public Service), 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 services, facilities and devices guideline.

Reporting inappropriate web content uploaded by students or employees

Any accidental access to inappropriate internet sites or where access to a site leads to inappropriate content must be reported by the teacher to their supervisor. The following actions must be taken by supervisors, managers, directors, principals or their delegate to remove and report the uploading of inappropriate images/footage, to websites (whether departmentally-owned or not), particularly where employees and students are involved or if the school is in some way implicated.

Step 1: Investigate the incident by reviewing the web content and determining the actions to be taken. If the website is blocked, contact the IT Service Centre by phone on 1800 680 445 to discuss options available, or escalate to the Cybersafety and Reputation Management Team on (07) 3034 5035, Cybersafety.ReputationManagement@qed.qld.gov.au for further investigation.

Step 2: If the content threatens or puts in danger staff, students or any community members, the principal follows the school's emergency response process and report the incident to the regional director.

Step 3: Immediately request the student/s or employee to remove content from the website, where possible. Alternatively, coordinate the removal with those directly involved or the website's service provider. Refer to the Cybersecurity and reputation management website (DoE employees only) and contact the Cybersafety and Reputation Management Team or the regional technology manager(DoE employees only) for assistance.

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 Integrity and Employee Relations (DoE employees only).

See the Advice for state schools on acceptable use of ICT facilities and devices for guidance.

Managed Print Services

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

- using the department's managed print service (DoE employees only), 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 (DoE employees only)
- 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
- authorising 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.

Closed Circuit Television and other video surveillance

When using Closed Circuit Television (CCTV), body-worn video or unmanned aerial cameras within their school, principals are to:

- carefully consider the location and position of cameras—as well as the technical specifications of the equipment chosen—to ensure the cameras only collect necessary and relevant personal information in a way that does not unreasonably intrude into someone's personal affairs
- take reasonable steps to make individuals aware of the purpose and legislative authority for collecting personal information (for example, place a prominent sign at the entrance to the camera surveillance system's area of operation and reinforce this with further signs near each camera)
- consider recordkeeping obligations under the *Public Records Act 2023* (Qld). Footage that is a public record must be retained for at least the minimum retention period specified in the Queensland State Archives' General Retention and Disposal Schedule (DoE employee only)
- only use personal information (surveillance footage where a person's identity is apparent) for the purpose for which it was obtained
- disclose surveillance footage containing personal information to law enforcement agencies, including the Queensland Police Service, only if it is 'reasonably necessary' for a law enforcement activity.

Network utilities

Principals are to ensure, where the school is using network utilities such as Closed Circuit Television systems, Light Emitting Diode (LED) signage and biometric devices, that they are placed on a separate Virtual Local Area Network (VLAN) if connecting to the departmental ICT network.

Email signature block

Employees are to ensure they add the departmental signature block to emails.

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 is not regularly backed up. This includes storing information on local hard drives (internal such as C: and D: drives or external) of computers or removable media.

Owners and/or 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, ICT Infrastructure Services, Information and Technologies Branch but at a minimum, on a monthly basis.
- maintaining a register of backups including verification of their success
- documenting and making available backup and restoration procedures
- providing the means to recover information by storing it at a 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
- considerations of appropriate technologies to ensure that backup data is able to be read if upgrades are made to the environment
- implementing a cycle of regular tests to verify that it can be recovered from the backups produced to meet requirements of the department's business continuity and ICT disaster recovery plans
- retaining a cycle of backup media of all information required to meet customer service, legal or statutory obligations
- the retention of backups is 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 the Queensland State Archives' General Retention and Disposal Schedule (DoE employees only)
- backup media to be disposed of in accordance with the Equipment management for business units procedure and Equipment management for schools procedure.

Metadata schemes

Owners and/or 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.

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

- Australian Government Locator Service (AS5044:2010) – is preferred for websites and is the minimum required metadata scheme for any ICT business system
- Australian Government recordkeeping metadata standard and guideline (National Archives of Australia) – 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 (Spatial Information Council) – is preferred for spatial data systems
- Metadata profile (National Digital Learning Resources Network - Education Services Australia) – ANZ-LOM metadata application profile.

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

- apply consistent metadata, use mechanisms such as controlled vocabulary, taxonomy, thesaurus (see below) (where applicable) 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, ensure the extension is implemented according to the metadata extension methodology in the scheme being used
- where applicable, ensure the metadata is extractable or exportable in an 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.

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

- Corporate thesaurus – Introduction (DoE employees only)
- Corporate thesaurus – Terms (DoE employees only)
- Business classification plan (DoE employees only) – quick guide to controlled vocabulary used for classifying, titling and indexing records.

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

- Australian Thesaurus of Education Descriptors (Australian Council for Educational Research) – definitive reference on Australian terminology in the area of education

- Schools Online Thesaurus (Education Services Australia) – a controlled vocabulary of terms used in Australian and New Zealand schools including educational and administrative processes
- Australian Public Affairs Information Service (National Library of Australia) – humanities and social sciences subject index
- Dewey Decimal Classification (Online Computer Library Centre) – library classification system.

The Director, ICT Infrastructure Services, Information and Technologies Branch assists in the implementation of metadata schemes for websites. The Director, Information and Governance Management, Information and Technologies Branch will advise on all other metadata applications in particular recordkeeping.

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:

- undergoes timely reviews and contains appropriate metadata and recordkeeping processes
- complies with the Queensland Government's Digital services policy and Consistent User Experience Standard (CUE) and Corporate Identity (see the department's Communication and marketing OnePortal web page (DoE employees only)), and the required compliance levels of the World Wide Web Consortium's Web Content Accessibility Guidelines
- contains contact information, privacy notices, provisions for customer feedback and information requests, disclaimer notices, and the appropriate Creative Commons licence.

All websites must be hosted within web hosting services authorised by the Assistant Director-General, Information and Technologies Branch. This includes websites for school activities as well as websites that an employee has created to support classroom activities.

School websites have a partial exemption from CUE and advice on this can be obtained from Web and Digital Production, Information and Technologies Branch. For more information refer to the Website publishing web page on OnePortal (DoE employees only) or contact your regional technology manager (DoE employees only).

Domain names

Employees, schools and, central and regional business units must ensure they use qld.gov.au or eq.edu.au for domain names. Non-government domain names are not to be used unless there is a compelling reason to do so and approval is received in accordance with this procedure.

Employees, schools and, central and regional business units who require new, changes, decommissioning, deregistration, exemptions etc. for a domain name, sub domain name or fifth level domain and/or web hosting services must log a request through Services Catalogue Online (DoE employees only). The request will be forwarded to Web and Digital Production 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 and Digital Production will advise and assist the school or regional office and the Director, Information and Governance

Management in the decommissioning of the website in accordance with the Information asset and recordkeeping procedure.

Domain names are to be promoted in advertising according to the Queensland Government's advertising requirements.

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 and Digital Production must approve all new domain names.

Exemptions from domain name and web hosting requirements under this procedure are sought by 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 or other form of school council.

The Director, Web and Digital Production is the nominated delegate as the single point of contact within the department for registrations with the Queensland Government domain provider. The role is also responsible for maintaining the department's central register of domain names with their renewal dates, registration details and passwords.

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 ID accounts for generic, employee and non-departmental users are managed through the iRegister system (DoE employees only).

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. 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 ensure details are kept up-to-date where work identification and location details are provided within a directory (e.g. phone directory).

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 the Identity (ID) and access management guideline are adhered to
- ensure that information about identities under domestic violence orders (including protection orders and temporary protection orders) is classified as PROTECTED and access is restricted in accordance with the Information security procedure
- 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. The MIS system is used to deactivate a student, where a student has left, had their enrolment cancelled, been suspended or excluded. If an account is to remain active the accountable officer is responsible for the actions that occurs within this account
- conduct quarterly reviews of account holders and communicate any required changes or updates to the status of the accounts to the IT Service Centre
- where temporary access is granted to non-departmental personnel, ensure that either:
  - effective controls are in place to restrict access only to information that is necessary to undertake their duties; or
  - they are continually supervised by a departmental user who has the appropriate authority to access the system.
- manage identities associated with their employees, such as renewing or deactivating accounts
- advise system administrators when employees commence duty, change their name and/or personal details, or leave the department
- inform owners and/or custodians 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.

Principals must also 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.

Owners and/or custodians accountable for a specified application or ICT business system must:

- 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 Privacy statements OnePortal web page (DoE employees only) for more information
- protect the identities of users, including students enrolled in schools who have become subject to legal orders, in such a way 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 owner and/or the 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 (including changes to access rights) and privileges are in accordance with Identity (ID) and access management guideline and in the case of schools match student enrolments
- implement audit logging with relevant internal controls, monitoring, reviewing and processing mechanisms commensurate with the information security classification level.

Software licence management

The department implements and manages the purchase, installation, maintenance and retirement of software and licences. To ensure compliance employees must:

- comply with the software's terms and conditions of use
- not breach any copyright or anti-piracy laws
- acquire, where possible, all software for departmental ICT devices through Services Catalogue Online (DoE employees only)
- 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 (DoE employees only) 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 Services Catalogue Online (DoE employees only).

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 purchased (regardless of method of purchase/acquisition) including ownership, allocation, site licences and any variations approved by the licence owner. This excludes any licence distributed as part of the department's managed operating environment (MOE)
- coordinate purchases in compliance with the Purchasing and procurement procedure through a Queensland Information Technology Contracting (QITC) framework accredited supplier

- ensure that software licences are procured under the name of 'The State of Queensland acting through the Department of Education'
- 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 Services Catalogue Online (DoE employees only)
- acquire any open source software (OSS) in accordance with QITC framework and ensure that use, modification and distribution adheres to the OSS licence conditions
- not use OSS where software applications have been mandated for whole-of-government use e.g. SAP Financial Management
- contribute or release any departmental OSS subject to a business assessment including legal review and appropriate copyright licence
- undertake an annual review of software compliance in their business unit or school (this excludes licences distributed under the MOE)
- ensure school managed bring your own device programs comply with software licensing conditions for non-departmentally owned device.

Executive Director, Enterprise Technology Services, Information and Technologies Branch is responsible for:

- processes for the management, maintenance, monitoring, reporting and retirement of enterprise software and their licences
- 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.

Definitions

Term	Definition
Custodian	Custodian may refer to an information custodian, data custodian or business system custodian or subject matter expert. Implements and maintains information assets and associated ICT resources according to the rules set in cooperation with the owner to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility throughout its lifecycle.

Term	Definition
Domestic violence order	A domestic violence order is made by a magistrate in court to stop threats or acts of domestic violence. There are two types of domestic violence orders: • protection order • temporary protection order.
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 devices	Electronic equipment designed for a particular communication and/or function.
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.
Information asset	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.
Non-departmental users	Persons who participate in departmental business processes but are not employees. For example, parents, medical service providers, work experience supervisors, pre-service teachers, community users and other government employees.
Owner	An owner authority and accountability for an information asset and associated ICT resources and approves the rules by which the asset is managed. Ownership is often delegated to the operational Assistant Director-General or Executive Director. Owner may be referred to as information owner, business system owner, application owner, or system owner.

Legislation

- *Right to Information Act 2009* (Qld)
- *Information Privacy Act 2009* (Qld)
- *Public Records Act 2023* (Qld)
- *Criminal Code Act 1899* (Qld)

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Nil

Supporting information for this procedure

- Advice for state schools on acceptable use of ICT facilities and devices
- Identity (ID) and access management guideline
- Use of ICT facilities and devices guideline

Other resources

- Queensland Government's Code of conduct for the Queensland public service
- Queensland Government's Digital services policy
- Information and Technologies (DoE employees only)
- Queensland Government's Use of internet and email policy
- Creative Commons licences guidelines
- Queensland Government's Consistent User Experience Standard
- Smartcopying Safe Harbours
- World Wide Web Consortium's Web Content Accessibility Guidelines
- Queensland Information Technology Contracting framework
- Information security procedure
- Information asset and recordkeeping procedure
- Non-departmental ICT service providers procedure
- Equipment management for business units procedure
- Equipment management for schools procedure
- Enterprise risk management procedure
- Purchasing and procurement procedure
- Privacy statements (DoE employees only)
- Queensland Government's Authorised and unauthorised use of ICT services, facilities and devices guideline
- Queensland Government's advertising guidelines
- Corporate thesaurus – introduction (DoE employees only)
- Corporate thesaurus – terms (DoE employees only)
- Business classification plan (DoE employees only)
- Services Catalogue Online (DoE employees only)
- Cybersafety and reputation management (DoE employees only)
- Investigations (DoE employees only)
- Managed print service (DoE employees only)
- Regional technology managers (DoE employees only)

- Purchase software for home use - Staff (DoE employees only)
- iRegister (DoE employees only)
- iSecurity (DoE employees only)
- Website publishing (DoE employees only)
- Queensland State Archives' General Retention and Disposal Schedule (DoE employee only)
- Australian Government Recordkeeping Metadata Standard
- Australian Government Locator Service (AS5044:2010)
- Australia and New Zealand Land Information Council
- Australian Government Recordkeeping Metadata Standard
- Metadata profile
- Australian Thesaurus of Education Descriptors
- Schools Online Thesaurus
- Australian Public Affairs Information Service
- Dewey Decimal Classification

Contact

For further information on ICT policies, procedures and standards please contact:
Governance Risk and Compliance unit
Email: ICTPolicy@qed.qld.gov.au

Review date

1/11/2018

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 Use of ICT systems

1.0 Information Communication and Technology (ICT)

Creative Commons licence