Procedure

Use of ICT services, facilities and devices procedure

Version: 2.0 | **Version effective**: 13/07/2026

Audience

Department-wide

Purpose

This procedure outlines the responsibilities and processes for the acceptable access and use of the Department of Education's (department) information and communication technology (ICT) services, facilities and devices. It provides guidance to schools on regulating employee and student use of ICT.

Overview

The department allows students and employees to access ICT services, facilities and devices for educational purposes and departmental business. Employees are committed to the acceptable use of departmental ICT and use it to undertake various activities directly or indirectly to perform their responsibilities. Principals monitor student use and access to these ICT services, facilities and devices.

Acceptable use of ICT includes professional development, business or school use and limited personal use. Inappropriate use of ICT by students or employees is reported and the relevant parties are notified.

The access and use of departmental ICT services, facilities and devices requires responsible management practices, education, training and employee accountability.

Use of departmentally provided ICT on privately-owned devices (such as accessing government email or Wi-Fi services) must comply with this procedure. However, the use of privately-owned devices more broadly is out of scope.

This procedure is supported by the:

- Advice for state schools on acceptable use of ICT services, facilities and devices
- Information and communication technology (ICT) policy
- Non-departmental ICT service providers procedure
- Use of ICT facilities, services and devices guideline (DoE employees only)

- Use of mobile devices procedure.

Responsibilities

Employees

- use ICT services, facilities and devices appropriately
- report inappropriate use of ICT to supervisor, manager, principal, director or above
- report suspicious or unsolicited ‘spam’ or ‘phishing’ emails
- acquire, install and use software in accordance with department procedures and software licences
- ensure department websites follow accessibility and usability requirements.

Managers, principals, directors or above

- assess and approve requests for user accounts to the department's ICT business systems limiting access where appropriate
- continually manage employee access to the department's ICT business systems and risks posed by unauthorised access to information
- resolve or progress incidents of employees’ inappropriate use of ICT
- manage the updates, licences, and fees to software that has been purchased in their business unit or school
- oversee the maintenance of a software asset register within the OneSchool Asset Register or SAP asset register
- where appropriate, review, remove and restrict access to websites or applications hosting inappropriate content which involves employees, students or implicates a school or the department
- retire, replace and coordinate the uninstallation of software
- undertake an annual review of software compliance in their business unit or school.

Principals

- oversee student access to the department's applications and ICT business systems
- assess and deactivate student accounts to the department's ICT business systems
- follow the school’s emergency response process if inappropriate web content uploaded to a website or application is a threat to employees, students or a community member
- monitor school websites and social media created for the purposes of school groups and activities.

Process

Managing access to ICT services, facilities and devices

The department controls and restricts access to its ICT business systems to prevent breaches and misuse. The following section outlines how the department manages ICT access for students and employees.

Employee access requests to ICT business systems

Employees may require access to several different ICT business systems to fulfil their role. Access to some systems will be granted when employees start with the department. To request access to ICT business systems:

- Employees use the iRegister system (DoE employees only) to request access to the department's ICT business systems and applications including the corporate VPN, EduWorkspace and some Microsoft 365 applications.
- Managers, principals, directors or above review access requests and must consider:
  - if an employee needs system access to fulfil their role (refer to Identity default access entitlements (DoE employees only) (KBA0019201) in Services Catalogue Online (SCO))
  - restricting access to information classified as PROTECTED following the Information security procedure.

For further information about requesting and managing access to departmental ICT business systems refer to the iRegister (DoE employees only) OnePortal page.

Other forms of access to ICT business systems

- If non-departmental users are given temporary access to ICT business systems, managers, principals, directors or above must either:
  - put in place controls so non-departmental users can only access the information they need to fulfil their role
  - have an appropriate departmental employee with system access supervise the non-departmental user.
- For schools, principals can approve the use of generic accounts from within iRegister considering the risks, benefits, cost, ongoing management and alternative options. See the Create a new generic account (DoE employees only) (KBA0018946) for more information.

Ongoing management of ICT business systems

- Managers, principals, directors or above who control access to an application or ICT business system must:
  - make sure user access application forms include a privacy collection statement that indicates how personal information is collected, will be used and protected. See the Privacy collection notices (DoE employees only) OnePortal page for information on privacy statements
  - educate employees and students annually (or when system updates require) about the password and security requirements of ICT business systems:
    - for password requirements see the Network Password Requirements help article (DoE employees only) (KBA0020064)
    - for security requirements see the Cyber security (DoE employees only) OnePortal page
  - immediately notify Business System Owners when an employee's access should be deactivated for unacceptable use of ICT business systems. Refer to the Use of ICT services, facilities and devices guideline (DoE employees only) for more details
  - disable or modify employee access to the relevant system if they:
    - resign

        - are seconded
        - take a prolonged period of leave
        - are dismissed or suspended
    - ensure ICT business systems are approved, managed and established following departmental processes and ICT standards
    - review employee access at least once every quarter making sure access levels are appropriate. If access needs to be updated and cannot be updated through iRegister, log a General enquiry request (DoE employees only) in SCO
    - continue to protect the identities of employees and enrolled students who have become subject to legal orders so only authorised employees (for example, manager, principal or delegate) have access
    - encourage employees to make sure their details are kept up to date where work identification and location details are provided within a directory.

Managing and deactivating a student's account

- Principals are responsible for overseeing student access to the department's applications and ICT business systems and:
    - must use the Managed Internet Service (MIS) (DoE employees only) to temporarily deactivate a student's access such as email and internet access if they are suspended, excluded, or due to their inappropriate use
    - must use OneSchool to manage changes to students' enrolment status
    - are responsible for the actions which occur on all active accounts, including those which should be deactivated.
- Principals may deactivate a student's account due to inappropriate use or for the duration of vacation periods by following the article Suspend/disable a student's identity (DoE employees only) (KBA0014976). They must use a risk assessment approach which considers:
    - the impact on the student's education or training outcomes
    - the likelihood the system or network will be used inappropriately
    - if the student has a history of inappropriate use
    - whether the student's need for access to complete course requirements outweighs the protection of the system or network.
- To disable a student account immediately, the principal should contact the school's technician or contact the IT Service Centre.

School ICT policy

- Principals must ensure a policy outlining the acceptable and legal use of departmental ICT is developed for their school. This can be added to the Student Code of Conduct information regarding the use of mobile phones and other devices, or can take the form of a procedure, policy, statement or guideline. The policy should also include information for students and parent/carers about student personal mobile device access. Further advice and a template are available within the Advice for state schools on acceptable use of ICT services, facilities, and devices.

- Principals must ensure the school's acceptable and legal use of ICT policy is understood and acknowledged by school students and parent/carers at least annually, either on the date of enrolment or through communication with parent/carers at the start of each school year.

Employee use of ICT services, facilities and devices

Employees access and use of departmental ICT is appropriate and aligns with the department's ICT policy, Code of Conduct and Standard of Practice. While personal use of departmental ICT is permitted, it must be limited, infrequent, undertaken when not working (such as lunch breaks or outside of scheduled work hours) where possible, and done without impacting other employees or the operation of government. However, personal use of departmentally owned mobile devices within a State Delivered Kindergarten (SDK) is restricted. Further information for SDKs is provided within the Safe use of digital technologies and online environments policy (DoE employees only).

Refer to the Use of ICT services, facilities and devices guideline (DoE employees only) for full details on acceptable and unacceptable use.

Acceptable use

- Employees' access to intranet, internet and network usage is monitored and email messages sent or received by anyone using the department's ICT business systems may be inspected to:
  - identify inappropriate use
  - protect system security
  - maintain system performance
  - protect the rights and property of the department
  - determine compliance with state, Commonwealth and departmental policy.

Limited personal use

- Employees' appropriate use of the department's ICT includes limited personal use (excluding the personal use of departmentally owned mobile devices within an SDK). Personal use includes checking personal social media, calling a family member on a desk phone, or completing study or personal banking. Employees must ensure personal use:
  - is infrequent
  - is done during off-duty hours, like lunch breaks or before or after work
  - does not disrupt government operations or incur additional costs to the department
  - does not disrupt their own or anyone else's work
  - does not extend to personal, financial or commercial gain.

Reporting inappropriate use

- Employees must report inappropriate use of ICT services, facilities or devices to their supervisor, manager, principal, director or above. Examples of inappropriate use include:
  - the access, creation, transmission or storage of pornographic, racist, violent, or any other unacceptable content

- to collect, access, use or disclose personal information for an unauthorised purpose
- use of gambling websites or applications
- installation or use of restricted applications such as TikTok and DeepSeek
- using their privately-owned email accounts for departmental business
- use of software in breach of the licensing conditions
- disabling or interfering with the operation of antivirus software
- attempting to bypass cyber security controls
- excessive personal use
- sharing passwords to ICT business systems or applications they can access.

- Once notified the supervisor, manager, principal, director or above must:
  - resolve the incident locally where possible
  - if the incident cannot be resolved locally, submit an Information security incident (DoE employees only) SCO form or contact the following (as appropriate):
    - for technology issues contact IT Service Centre on 1800 680 445 or SCO (DoE employees only)
    - for a privacy breach to the Privacy team using the Report a privacy breach (DoE employees only) SCO form in accordance with the Privacy data breach and complaints procedure
    - for violations of the Queensland Government's Code of Conduct for the Queensland Public Service contact Integrity and Employee Relations.

If the department reasonably suspects an employee's misuse of the network may be misconduct, corruption, or a criminal offence under section 426(4A) of the *Education (General Provisions) Act 2006* (Qld), it will report the case to the police.

Report suspicious emails

- Employees may receive suspicious or unsolicited 'spam' or 'phishing' emails which:
  - ask for sensitive information, such as bank details
  - encourage people to open a malicious attachment
  - link to a fake website which asks for sensitive information or downloads malicious content without a user knowing.
- If employees receive a suspicious email, they must report it and avoid clicking on any links they contain.
- Employees report suspected 'spam' or 'phishing' emails to the Cyber Security Operations team by using the 'Report' button located in the Outlook toolbar or by forwarding the email as an attachment to operational.security@qed.qld.gov.au.

Reporting inappropriate web content accessed or uploaded by students or employees

Supervisors, teachers, managers, principals, directors or their delegate must follow this process to remove and report inappropriate content uploaded to any websites or applications (whether departmentally-owned or not), particularly if employees and students are involved or the school or department is implicated in some way.

This includes content uploaded on privately-owned or departmental devices and situations where the content identifies the person as an employee (or student, parent/carer etc.). Any accidental access by a student or employee to inappropriate sites or where access to a site leads to inappropriate content must be reported to their relevant supervisor, teacher, manager, principals, directors or their delegate for review.

Supervisors, teachers, managers, principals, directors or their delegate review the web content (where accessible) and determine the actions to be taken.

- If the website or application is blocked by the department's network:
  - contact the IT Services Centre by phone (1800 680 445) to discuss available options
  - contact the Cybersafety and Reputation Management Team (07 3034 5035), or
  - log a Cybersafety enquiry (DoE employees only) SCO form for further investigation.
- If the content poses a threat to school employees, students or any community member the principal follows the school's emergency response process and reports the incident to the Regional Director.
  - School, regional or central office employees who need to contact local law enforcement must refer to the Disclosing personal information to law enforcement agencies procedure and complete a Disclosure of personal information to a law enforcement agency (LEA) form.
- Supervisors, teachers, managers, principals, directors or their delegate must facilitate the removal of the content and:
  - where possible, direct the student or employee responsible for uploading the content to remove it from the website or application
  - coordinate the content's removal with the website/application owner or service provider:
    - content hosted on social media can be directly reported on the hosting page
    - content hosted on other websites will need to be removed directly by their owners. The owner's details can normally be found on the bottom of the web page
  - if further assistance is required:
    - refer to the Remove harmful online content (DoE employees only) SCO form
    - contact the Cybersafety and reputation management team (DoE employees only) or their IT Customer Manager (DoE employees only).
- Supervisors, teachers, managers, principals, directors or their delegate must minimise access to the offensive content:
  - schools can contact their Managed Internet Service administrator (DoE employees only) to immediately 'block' the website or application at the school level
  - regional and central office can use the Unblock or block a website (Corporate) (DoE employees only) SCO form to request a departmental 'block'.
- If personal information has been uploaded supervisors, teachers, managers, principals, directors or their delegate must contact the Privacy Team and refer to the Privacy data breach and complaints procedure.
- Supervisors, teachers, managers, principals, directors or their delegate should report any incident that has grounds for discipline and meets the threshold for misconduct (as defined in the Public Sector Act 2022 (Qld)) to the Integrity and Employee Relations unit.

- schools can report the incident via iRefer (DoE employees only)
- regional and central offices can report the incident by:
  - sending an email to intake@qld.gov.au
  - calling 1800 468 253
  - via mail to: Manager, Intake and Assessment, Department of Education, PO Box 15033, City East, Qld, 4002.

For school specific ICT responsible use requirements refer to the Advice for state schools on acceptable use of ICT services, facilities and devices.

Software applications and software licences management

All software, including free and open-source software (OSS), must be purchased, installed or implemented, used and managed in compliance with this procedure and any licensing terms and conditions that may restrict where and how it is used.

Using unauthorised or unlicensed software, or violating software licensing terms of use, can present reputational, legal and cyber security risks to the department and its employees. To minimise these risks, follow the steps below.

Purchasing and installing licensed software

All employees must:

- not install, or attempt to install, unlicensed or unauthorised software on any departmental ICT devices
- acquire all online services in line with the Non-departmental ICT service providers procedure
- seek approval from a manager, principal, director and above to purchase or obtain software licenses
  - specific instructions and forms for requesting some software, such as Adobe Creative Cloud, are available through the Software and business systems (DoE employees only) in SCO
- install software on departmental ICT devices using the appropriate software request form on SCO (DoE employees only). If no dedicated form exists, use the General software (DoE employees only) SCO form.

Teachers, managers, principals, directors and above must:

- coordinate purchases in compliance with the Purchasing and procurement procedure and ICT asset management procedure
- ensure that software licences are procured under the name of 'The State of Queensland acting through the Department of Education'.

Using and managing licensed software

All employees must:

- understand and follow their obligations under the licensing terms and direct any software licence enquiries such as compliance and eligibility using the General enquiry (DoE employees only) SCO form
- ensure free software for privately-owned devices such as Microsoft Office 365 (DoE employees only) and Adobe Creative Cloud (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

- notify a supervisor, manager or above about unlicensed or unauthorised software (including any privately-owned) on departmental ICT devices that needs to be uninstalled
- ensure privately-owned mobile devices connected to the department's network have appropriate licenses for the software being used.

Teachers, managers, principals, directors and above must:

- manage licensed software in accordance with the ICT asset management procedure
- take full responsibility for the management of directly purchased software, including updates, licensing, fees and compliance to its terms and conditions of use
- maintain a Software asset register (DoE employees only) to monitor, record and manage software use (including the storage of original media and licence documentation, but excluding licences distributed as part of the department's managed operating environment (MOE)). To register software assets:
  - schools use the OneSchool Asset Register (DoE employees only)
  - regional and central offices use SAP asset register (DoE employees only)
- coordinate an annual review of software compliance in their business unit or school (this excludes licences distributed under the MOE)
- coordinate the uninstallation of software identified as unlicensed, unauthorised, inappropriate or deemed as an unsupported application using a General software (DoE employees only) SCO form
- ensure school managed bring your own device programs comply with software licensing conditions for privately-owned devices.

Considerations for open-source software (OSS)

All employees must:

- not use OSS applications where whole of government applications have been mandated for use, such as SAP financial management
- undertake a business impact assessment which includes advice from Legal Services and the appropriate copyright licence before contributing to or releasing any departmental OSS.

Teachers, managers, principals, directors and above must:

- acquire any OSS in accordance with the Queensland Government's Open source software guideline and seek Software licensing team approval (DoE employees only) (KBA0018403) before installing it on departmental devices
- ensure that use, modification and distribution of OSS software adheres to the OSS licence conditions.

Departmental websites

All departmental websites must be hosted on web hosting services authorised by the Assistant Director-General (ADG), Digital Products and Assurance. This includes websites created to support school and classroom activities.

- Employees with permission to edit content on school or corporate websites must ensure the website follows accessibility and usability requirements consistent with Queensland Government standards and branding guidelines. This includes:
  - regularly reviewing and updating content so it remains current and accurate
  - appropriate metadata and records management processes
  - following the Queensland Government's Digital service policy and the Web Content Accessibility Guidelines
  - providing contact information, privacy notices, provisions for customer feedback and information requests, disclaimer notices, and the appropriate Creative Commons licence.
- Principals are responsible for their school's web publishing. School based employees can request access to edit content on their school website or request website support via the Websites for Schools support (DoE employees only) SCO form. The relevant principal must approve these requests within SCO where required.
- Principals are also responsible for monitoring websites and social media created for the purposes of school groups and activities, such as Parents and Citizens' associations and sporting groups, to ensure users maintain appropriate privacy and respectful interactions. For further guidance refer to the Social media for school and departmental promotion procedure or the Queensland Government's Principles for the use of social media networks and emerging technologies.
- Employees in corporate business units can log a request to publish, update or remove content they are responsible for on departmental websites via a Web work request (DoE employees only) SCO form. The approvals required depend on the nature and urgency of the request, for more information refer to the Web work request (DoE employees only) OnePortal page.
- Employees can request an investigation into whether the Web Content Accessibility Guidelines or web content quality assurance reviews apply to their situation via the Quality assurance requirements assessment (DoE employees only) SCO form.
- Web and Digital Production (WDP) (DoE employees only) unit can provide advice on web content publishing and web-based solutions for both corporate business units and state schools. For more information refer to the OnePortal Website publishing page (DoE employees only) or schools can contact their IT Customer Manager (DoE employees only).

Use of domain names

Employees must use the correct domain name (e.g. qld.gov.edu.au) when creating a website or application. All new domain name requests (including sub domain names or domains five levels deep in the hierarchy) must be reviewed and approved by WDP.

Requesting a new domain name

- Employees seeking a new domain name must contact WDP via domainname.admin@qed.qld.gov.au. WDP will assess this request to:
  - ensure the correct domain name is used, or that an exemption has been provided (see below)
  - determine whether associated costs apply (schools are not required to pay for their primary domain name but additional domain names may incur a cost)

- ensure the approved process has been followed.

- WDP will respond to the requestor and, if approved by the Director, WDP, will manage the submission with the domain name provider.
- Employees must promote domain names in accordance with the Queensland Government's Domain name registration and management standard to ensure advertising and sales collateral is not ordered until the domain name has been secured.
- The Director, WDP is the nominated delegate as the single point of contact within the department for registrations with the Queensland Government domain provider.

Exemptions

- Employees can seek exemptions from the department's domain name requirements by submitting a business case to the ADG, Digital Products and Assurance for approval. The submission must:
  - be in the form of a general briefing note
  - outline why an exemption is needed.
- The ADG, Digital Products and Assurance will assess the submission and approve or deny the request.

Decommissioning a domain name

- If employees want to de-register or decommission a domain name, related website or application they can seek advice from WDP. WDP will assist the school, regional office or business unit with the decommission process in accordance with the Records management procedure.

Backing-up information stored on ICT devices and business systems

- Employees must not store the only copy of important information on storage media that is not regularly backed up such as local hard drives (internal such as C: and D: drives or external) of computers or removeable media. Network drives and departmentally authorised recordkeeping systems are regularly backed up by the department.
- Business System Owners who locally manage ICT business systems and applications will need to follow backup rules and set controls as outlined in the Use of ICT services, facilities and devices guideline (DoE employees only).

Definitions

Term	Definition
Authorised recordkeeping systems	An ICT business system designed to capture, manage and provide access to records through time, that is intended to preserve the context, authenticity and integrity of the records. Authorisation is provided by a principal, an executive director or above, ensuring compliance with recordkeeping requirements such as Public Records Act 2023 (Qld) and Queensland Government's Records governance policy. Examples of approved recordkeeping systems include Content Manager for regional and central offices, the OneSchool (DoE employees only) suite of applications for schools or suitable secure file location on school servers.

Term	Definition
	ICT business systems that do not qualify as an authorised recordkeeping system include email systems (such as Outlook), OneDrive, Teams, QChat. Further information can be found in OnePortal under Records management (DoE employees only).
Business System Owner	An employee who has 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 For example, the Director of Enterprise Information Services is the Business System Owner for Content Manager and the Principal of a school is the Business System Owner for IDAttend.
Employee	Any permanent, temporary, seconded, casual or contracted staff member, contractors and consultants or other person who provides services on a paid 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 department, heads of curriculums, guidance officers, teachers and other school staff. Volunteers depending on the engagement may not be considered employees but should have regard for this procedure.
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. They include ICT services, facilities and devices.
ICT devices	Electronic or digital devices/equipment designed for a particular communication and/or function, including but not limited to computers, mobile devices, television sets, interactive panels and boards, gaming/esports (DoE employees only) consoles and equipment, augmented or virtual reality equipment, AV/media streaming and storage devices, and digital or analogue records such as DVD and video, photocopiers/printers and other imaging equipment.
ICT facilities	An electronic capability designed for a particular communication and/or function, which includes but is not limited to electronic networks, online environment, internet, extranet, email, instant messaging, artificial intelligence (AI) including generative AI, webmail, fee-based web services and social media.
ICT services	Telecommunications services that carry voice and/or data and includes applications, hosting, storage, and cloud-based services etc.
IT Customer Manager	IT Customer Managers (DoE employees only) are part of Customer Engagement within Digital Innovation Division. Their responsibilities include

Term	Definition
	communicating and directing policies, plans and services within schools, supporting schools with strategic planning, gathering requirements for future services and products within schools, capturing feedback and managing expectations of schools.
Mobile device	A portable digital computing or communications device with information storage capability that can be used from a non-fixed location. Mobile devices include, but are not limited to, mobile and smart phones, smart watches and wearable devices, 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.
Online services	Online (or digital) services are websites, web applications and mobile applications that are delivered over the internet or require an internet connection. They are used to meet a range of needs for education, collaboration and connectivity for students and employees. Examples of online services include interactive learning sites and games, online collaboration and communication tools, web-based publishing and design tools, learning management systems, file storage and collaboration services. They can be free or paid subscriptions and may or may not be provided by the department.
Open-source software	Open-source software is software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. Open-source software is made by many people and distributed under licenses that comply with the Open Source Definition.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: • whether the information or opinion is true or not, and • whether the information or opinion is recorded in a material form or not.
Privately-owned 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 privately own the device. Also known as a personal electronic device. It also includes bring your own device (BYOx) initiative.

Legislation

- *Criminal Code Act 1899* (Qld)
- *Education (General Provisions) Act 2006* (Qld)
- *Information Privacy Act 2009* (Qld)

- *Public Records Act 2023* (Qld)
- *Public Sector Act 2022* (Qld)

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Information and communication technology (ICT) policy
- Non-departmental ICT service providers procedure
- Use of mobile devices procedure
- ICT asset management procedure

Supporting information for this procedure

- Advice for state schools on acceptable use of ICT services, facilities, and devices

Other resources

Department of Education

- CCTV use in schools procedure
- Code of conduct for the Queensland public service
- Cyber security (DoE employees only)
- Disclosing personal information to law enforcement agencies procedure
- Equipment management for business units procedure
- Equipment management for schools procedure
- ICT standards (DoE employees only)
- iRegister (DoE employees only)
- IT Customer Manager (DoE employees only)
- Managed Internet Service (DoE employees only)
- OneSchool Asset Register (DoE employees only)
- Orange Card Holders (DoE employees only)
- Reporting spam or phishing emails (DoE employees only)
- Safe use of digital technologies and online environments policy (DoE employees only)
- SAP asset register (DoE employees only)
- Services Catalogue Online (SCO) (DoE employees only)
- Social media for school and departmental promotion procedure

- Use of ICT services, facilities and devices guideline (DoE employees only)

Whole of government

- Digital services policy
- Domain names policy
- Domain name registration and management standard
- Open source software guideline
- Principles for the use of social media networks and emerging technologies
- Use of internet and email policy

External

- World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG)

Contact

For further information on ICT policies and procedures contact:
Governance Risk and Compliance unit,
Digital Innovation Division
Email: ictpolicy@qed.qld.gov.au

Review date

13/07/2029

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 Use of ICT systems procedure

Creative Commons licence

Attribution CC BY

Refer to the Creative Commons Australia site for further information