Policy and Procedure Register updates

Summary of changes to:

Information and Communication Technology (ICT) policy

1. Reason for new/updated policy or procedure *(select all that apply)*		
☒ Change of policy/procedure requirements	☐ Audit/review recommendation	
☒ Change to legislation/delegations	☐ Due for review	☒ Other - New

The new Information and Communication Technology (ICT) policy (the policy) was created to provide the Department of Education's (the department) intent, commitments and requirements for the use, management and investment of ICT.

The policy is the overarching policy for the following procedures:

- Use of ICT systems procedure (under review)
- Non-departmental ICT service providers procedure (under review)
- Use of mobile devices procedure (under review)
- ICT asset management procedure.

The policy incorporates the ICT asset management policy which will be removed on publishing.

2. Summary of changes

The policy is new to the PPR and consolidates the existing procedure and whole of government and legislative requirements. It includes sections for the Access and use of ICT, Management of ICT, and ICT investment.

The Access and use of ICT section highlights key legislation and procedure requirements to ensure employees and students are using the department's ICT responsibly, ethically, equitably and legally. The information outlining how the department meets ICT security requirements, manages personal information and protects and maintains privacy aligns with recent amendments made to the *Information Privacy Act 2009* (Qld).

Management of ICT states how the department governs, manages and monitors its ICT and software, including artificial intelligence (AI) tools, throughout their lifecycle. The approvals required to store or process data or information offshore are included and align with the Queensland Government's Information security classification framework.

ICT investment encompasses the requirements and procedures for acquiring online services and ICT investments. Online services undergo information security, privacy and online safety assurance processes before procurement.

3. Impacts to roles and responsibilities

Does the new/updated content change staff roles/responsibilities *in any way*?	☒ Yes	☐ No

If yes, select the type of change: *(select all that apply)*

☒ Revised responsibilities	☐ New/additional responsibilities	☐ Removed responsibilities

Position title	**Summary of change**	**Page#**

All employees	Clear high-level principles for accountability and responsibility, confidentiality and privacy, security and governance of ICT.	2
All employees	Includes legislative drivers behind employee responsibilities and the actions required to meet these responsibilities.	2-4

4. Communication and support for implementation

Changes to the policy have been communicated with the relevant internal stakeholders. Consultation was conducted across the department and included input from subject matter experts and relevant directors within the Digital Innovation Division (DID).

Department wide communication via OnePortal and ConnectEd will be developed in consultation with the DID communication team.

For further assistance, please contact:

- Policy/procedure contact:

  Governance, Risk and Compliance unit, Digital Innovation Division

  ictpolicy@qed.qld.gov.au

Policy

Information and communication technology (ICT) policy

Version: 1.0 | **Version effective**: 13/07/2026

Audience

Department-wide

Purpose

This policy outlines the Department of Education's (the department's) commitment to providing information and communication technology (ICT) services, facilities, and devices to support, enable and enhance its activities. The policy also establishes the department's position on the acceptable use of ICT services, facilities and devices.

Policy statement

A clear approach to the use and management of ICT empowers the department and its staff to use ICT appropriately, responsibly and effectively; maintain the security of the department's systems and the private information it holds; and optimise the investment and management of ICT across its lifecycle.

The department is committed to building its digital capability by effectively using ICT for teaching and learning, to modernise operations, and provide ICT support. Access to ICT services, facilities and devices is provided to employees, students and affiliates to undertake learning and departmental business and for limited community use.

The department is committed to providing safe, secure and appropriate ICT resources and services. It invests in digital services and capabilities to improve collaboration and innovation. Systems, solutions and processes are modernised to improve service delivery and maintain reliable, secure and scalable ICT solutions.

The use of privately-owned ICT is out of scope for this policy, however the access to and use of departmentally provided ICT while using a privately-owned device (such as accessing government email or Wi-Fi via a privately-owned device) is in scope.

Principles

Principle	What this means for the department
Accountability and responsibility	• All staff understand their responsibilities and obligations when using ICT. • Personal use of ICT is limited and does not disrupt the efficient delivery of department services. • All staff are empowered with tools and knowledge (DoE employees only) to make decisions relating to local ICT assets and online services. • The department provides transparency and assurance in its ICT investment decisions.
Confidentiality and privacy	• The department protects its ICT services and devices to safeguard privacy and confidentiality, preserve data and ensure the ongoing availability of information.
Security	• Security policies, controls and guidelines are enforced for storing, accessing, processing or transmitting data to safeguard against loss, unauthorised access, modification, disclosure and any other forms of misuse. • Online services undergo comprehensive assurance processes and can store and manage department information in line with their security classification.
Governance	• The department actively manages and monitors its ICT, including software and software licences, through a lifecycle approach. • The department supports safer use of third-party online services through assessment of information security and privacy compliance. • The department monitors its ICT for inappropriate use.

Requirements

The department adheres to the Queensland Government Enterprise Architecture (QGEA) as required under the Financial Performance Management Standard 2019 (Qld). Through this policy and its underlying procedures, the department aligns with key aspects of the QGEA as they relate to the management of ICT. This fosters a cohesive and standardised approach to ICT use and management across the department.

Access and use of ICT

Department employees use and access ICT in accordance with the Code of Conduct for the Queensland Public Service, the department's Standard of Practice, the Public Service Commission's directives and policies, related state and commonwealth legislation, such as the *Criminal Code Act 1899* (Qld), and the specific terms and conditions of the accessed service, facility or device.

The department controls and restricts access to its ICT to prevent breaches and misuse. Employee access to the department's ICT is regularly reviewed to ensure they can only access the information they need to fulfil their duties.

Student access to ICT can also be modified or restricted in response to inappropriate use. This allows the department to meet its security requirements, manage personal information and protect and maintain privacy in accordance with the *Information Privacy Act 2009* (Qld).

Employees complete training and access related support for the use of ICT relevant to their role.

The department uses licensed and authorised programs appropriately and complies with the terms of their licence in accordance with the *Copyright Act 1968* (Cwth).

Online services including applications are accessed by employees and students through the department's ICT have been assessed against a national framework and departmental standards. The assessment outcomes of online third-party services available for use in schools are published in the Online Service Risk Review Catalogue.

Mobile devices provided by the department are handled properly in accordance with the Use of mobile devices procedure.

Together these measures allow the department to ensure its ICT is used responsibly, ethically, equitably and legally.

Management of ICT

ICT is managed across the department to enable digital capability and competency. The department aligns with the relevant legislation, policy and whole-of-government requirements outlined in the QGEA and Financial and performance management standard 2019 (Qld). Projects are managed in line with the department's Enterprise portfolio and planning (DoE employees only), ensuring the business function is supported and streamlined in a cost-effective manner.

ICT assets are governed using the asset lifecycle approach defined within the ICT asset management procedure, including planning, purchasing and disposal. The lifecycle approach is regularly reviewed to ensure it continues to effectively manage the department's ICT assets and support the efficient delivery of frontline and corporate services.

All software is managed in accordance with the Queensland Government Software asset management policy and the department's Use of ICT services, facilities and devices procedure. The department effectively manages the purchase, installation, maintenance and retirement of enterprise software and software licences. This allows the department to easily track software licence requirements, account for maintenance renewal dates and upgrades, and plan for the timely and ordered retirement of its enterprise software.

The department monitors the use of ICT to ensure appropriate use in accordance with the Use of ICT services, facilities and devices guideline (DoE employees only). It oversees and reports on intranet, internet and network usage and inspects email messages sent or received by anyone using the department's ICT business systems. By monitoring ICT, the department can identify inappropriate use, security and privacy risks to the department's network, integrity and safety in compliance with federal, state and departmental policies. This allows the department to protect the security of its systems and maintain their performance.

If the department reasonably suspects an employee is using the department's network in a way which, after internal investigation and process, meets the threshold for misconduct, corrupt conduct or criminal reporting it will refer the matter to the police as per section 426(4) of the *Education (General Provisions) Act 2006* (Qld).

The department manages artificial intelligence (AI) tools throughout their lifecycle by adhering to the requirements of the Queensland Government's Artificial intelligence governance policy. AI tools are evaluated ensuring transparency, accountability and identification of risks.

Data or information that is stored or processed offshore is approved in accordance with the Queensland Governments Information security classification framework and the department's Non-departmental ICT service providers procedure. The security classification of the data or information determines the level of approval required.

ICT investment

The department plans and manages its purchasing of ICT in line with the requirements outlined in the Purchasing and procurement procedure. This contributes to the department's ability to provide transparency and assurance in ICT investment decisions.

Online services are acquired following the Non-departmental ICT service providers procedure. This ensures the use of enterprise services is prioritised. ICT related risks and issues are considered when determining suitability of acquiring an online service. Online services undergo information security, privacy and online safety assurance processes before procurement. These processes align with compliance requirements for the management of data, information and records in accordance with the *Public Records Act 2023* (Qld) and other legislative requirements. Part of this process consists of assessing whether online services have the appropriate controls and risk mitigation strategies to store and manage department information in line with its security classification.

ICT investments, including all software, are managed using a defined lifecycle beginning with planning for investment and ending with enhancing or retiring assets. The ICT asset management procedure outlines all five stages of the lifecycle and assists staff to meet their obligations under the Financial and Performance Management Standard 2019 (Qld). The lifecycle accounts for risk management, industry best practice and manufacturer standards. The department's lifecycle approach allows it to proactively plan for the ICT needs of business units and schools supporting them to meet compliance requirements and access the tools they need to deliver high quality front-line and corporate services.

Definitions

Term	Definition
Employees	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.

Term	Definition
ICT asset	ICT hardware, software, systems and services including voice, video and unified communication such as telephony and collaboration systems that are used in the department to process, store or transmit information such as computers, telephone systems, closed circuit television (CCTV) and video surveillance systems, servers, switches, wireless network equipment, cabinets, scanners, multifunctional printers, mobile phones, portable devices, digital cameras, electronic whiteboards, projectors, etc.
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 service	Telecommunications services that carry voice and/or data and includes applications, hosting, storage, and cloud-based services etc.
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.

Legislation

- *Copyright Act 1968* (Cwth)

- *Criminal Code Act 1899* (Qld)
- *Education (General Provisions) Act 2006* (Qld)
- Financial and Performance Management Standard 2019 (Qld) (section 23)
- *Human Rights Act 2019* (Qld)
- *Information Privacy Act 2009* (Qld)
- *Public Records Act 2023* (Qld)
- *Public Sector Act 2022* (Qld)
- *Public Sector Ethics Act 1994* (Qld)

Delegations/Authorisations

- Financial and administrative delegations (DoE employees only)
- Purchasing and procurement delegations (DoE employees only)

Policies and procedures in this group

- Use of ICT services, facilities and devices procedure
- Non-departmental ICT service providers procedure
- Use of mobile devices procedure
- ICT asset management procedure

Other resources

Department of Education

- CCTV use in schools procedure
- Code of Conduct and Standard of Practice
- Financial Management Practice Manual (DoE employees only)
- ICT asset management (DoE employees only)
- Information management, privacy and security policy
- Use of ICT services, facilities and devices guideline (DoE employees only)

Queensland Government

- Artificial intelligence governance policy
- Digital services policy
- ICT asset disaster recovery planning guideline
- ICT resources strategic planning policy
- Information security classification framework (QGISCF)

- Open data, information sharing, access and use policy
- Software asset management policy

Contact

For further information, please 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.

Nil

Creative Commons licence