Policy and Procedure Register updates

Summary of changes to:

Information security procedure

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

The Information security procedure (the procedure) was due for review on 1 June 2020. Updates have been made to simplify the process for employees to apply security classifications, protect information and report incidents or breaches.

The updates aim to provide employees with clear examples of how they must protect information as well as when and how to respond to an information security incident or breach.

This procedure is supported by the Information security guideline.

2. Summary of changes

The procedure has been updated to align with PPR requirements.

The process sections within the procedure have been condensed into 4 sections which are:

- Determine the information security classification (formerly ICT security)
- Apply and control the information security classification (formerly Applying information security classifications)
- Protect information (formerly Protecting information and Malware and malicious code prevention)
- Respond to information security incidents and breaches (formerly Breach of security and Reporting ICT security incidents).

The Protect information section has been rewritten to provide employees with clear, actionable steps to protect information, including malware prevention and clear desk/clear screen practices.

The Responding to information security incidents and breaches section now includes privacy data breaches.

Inclusion of a new Information security classification tool will assist employees in the classification of information assets to align with the Queensland Government's Information Security Classification Framework (QGISCF).

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#**

Employees	Employees now must report suspected or discovered privacy breaches. Some key process responsibilities were missing from the previous version of the procedure. These have now been included but do not represent new obligations.	4
System security administrators	Direct responsibilities for the prevention of malware and malicious code have been removed from this procedure and will now be outlined in the new iSecurity website.	5
Information Security Services unit	Direct responsibilities for protecting information have been removed from this procedure and will now be outlined in the new iSecurity website.	3-4
Enterprise Technology Services unit	Direct responsibilities for monitoring the system's capacity have been removed from this procedure and remain a business unit responsibility.	

4. Communication and support for implementation

Changes to the procedure have been communicated with the relevant internal stakeholders, with consultation conducted across the department, including 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
  Email: ictpolicy@qed.qld.gov.au

Procedure

Information security procedure

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

Audience

Department-wide

Purpose

This procedure outlines how the Department of Education (the department) protects its data, information, and information and communication technology (ICT) business systems against loss, inappropriate release, unauthorised access or use, accidental modification, and information security incidents.

Overview

This procedure details how employees are to protect and appropriately access information in their care and apply suitable controls when needed as per the *Criminal Code Act 1899* (Qld).

The department develops, implements, maintains and continually reviews appropriate security controls and processes in compliance with Queensland Government's information security related policies, ICT security processes and practices, reporting and auditing requirements, and legislative instruments.

The department supports employees to implement this procedure and provides mandatory competency-based training and education content available through the Education Futures Institute (EFI) Catalogue's including the Information security training (DoE employees only).

This procedure is supported by the:

- Information management, privacy and security policy
- Information classification and handling security guideline (DoE employees only)
- Information security classification (DoE employees only) OnePortal page
- Privacy data breach and complaints procedure.

Responsibilities

Employees

- protect and secure the department's information, ICT services, facilities and devices by accepting responsibility for information in their care

- determine the information security classification to information in their care and apply appropriate controls to prevent misuse, or unauthorised access or release
- take suitable precautions to prevent unauthorised access or release of information according to its information security classification
- only access information they are authorised to
- report all suspected or discovered information security incidents or breaches, or privacy data breaches.

Supervisors, managers, principals, directors and above

- promote staff awareness of their obligation to protect and secure the department's information and ICT services, facilities and devices
- assist employees to determine the appropriate information security classification and controls
- support schools, regional and central offices in the implementation of clear security control processes including roles and responsibilities for handling and managing of SENSITIVE or PROTECTED information.

Process

Determine the information security classification

Employees must understand the information security classification of the information, data or ICT business systems in their care. An information security classification determines how information, data and ICT business systems must be stored, managed, shared and released. Consistent and correct management secures against loss or inappropriate release.

Employees must determine which of the following three information security classifications apply:

- **OFFICIAL**: Used for non-sensitive information of a routine nature such as the street address of a school, a media release, or information that has been authorised to be released into the public domain. Information under this classification has no special sensitivity or handling requirements.
- **SENSITIVE**: Used for confidential information of medium sensitivity which is restricted to authorised persons on a 'need to know' basis. For example, an employee's home address, credit card or payment details, or medical information.
- **PROTECTED**: Used for confidential information of high sensitivity which requires a substantial degree of protection and restriction only accessible by authorised persons on a 'need to know' basis. For example, student protection information, court orders and Cabinet information.

If employees cannot easily determine an information security classification, they can find additional information in the Information classification and handling guideline (DoE employees only). Information assets are classified using the Information security classification tool (DoE employees only). Managers, principals, directors or above can assist in assessing the information security classification of any data, information or ICT business system.

Where the department receives and holds information that is owned or created by another government department, employees must maintain and not change the classification applied by the owning or creating department.

Apply and control the information security classification

Employees must protect information in their care according to its information security classification. This includes maintaining its confidentiality by restricting who can see it, ensuring its integrity by keeping it accurate and complete, and making it available so it can be accessed and used by the right people at the right time.

- Apply the information security classification as a label or text as appropriate to the ICT business system, information and/or mobile media in which the information is being stored. For example:
  - electronic documents can have an information security classification displayed on the front page, in a watermark, or the header or footer, and in the accompanying metadata or document properties
  - Content Manager files and folders have the information security classification set in their properties and associated 'Access Control' applied for SENSITIVE or PROTECTED files.
- Protect information within mobile devices as per the Use of mobile devices procedure including encrypting USB flash drives and portable hard drives.
- If the information is SENSITIVE or PROTECTED employees should apply reasonable precautions, such as restricting access to and encrypting information in storage, to protect it against illegal or unauthorised access, use, disclosure, modification, duplication, disruption and/or destruction.
- If the information security classification of an information asset needs to be changed, submit a Records management enquiry (DoE employees only) SCO form to assist.

For more information on applying and controlling information, and the environment in which it must be managed, see the Information classification and handling guideline (DoE employees only).

Protect information

Employees must:

- store mobile devices (such as laptops or mobile phones) and removeable media (such as USB flash drives) in lockable containers or a secure locked room
- ensure mobile devices are protected by means of strong passwords which are stored securely and not shared with others
- keep a clear desk and clear screen to protect and secure the department's information in their care by:
  - clearing desks of all SENSITIVE or PROTECTED materials (including sticky notes, notebooks and other physical documents) and mobile devices at the end of each day
  - locking unattended computers and mobile devices or logging off if left for an extended period of time
  - referring to the iSecurity website (DoE employees only) for more details on the department's clear desk and clear screen practices
- connect departmentally-owned devices to the network for software updates at least weekly, where possible
- only access and share information required to do their job
- protect the department's network and ICT from viruses, malware attacks, or malicious code by:
  - appropriately using their departmental issued user accounts and corresponding access
  - keeping the operation of antivirus software active

  - not breaching or bypassing information security protections, such as malware prevention and software controls
  - not developing, distributing or running any computer programs or code that is intended to replicate itself, cause damage, or impede the performance of any computer, software application or network
- immediately follow the Responding to information security incidents and breaches section below if a device has signs of malware attack such as frequent freezing or crashing, files suddenly changing or disappearing, or unusual or suspicious error messages
- dispose of documents and erase removable storage media containing SENSITIVE or PROTECTED information by using the Information classification and handling guideline (DoE employees only).

Supervisors, managers, principals, directors or above must:

- establish business unit or school security control processes including roles and responsibilities for handling and managing of SENSITIVE or PROTECTED information, and incorporate these into position descriptions and performance agreements
- provide induction and on-going information security training for employees using resources such as the Information security course (DoE employees only) in the EFI Catalogue
- ensure employees and other authorised people only access departmental information and systems with the minimum-security access necessary to fulfil their role
- undertake an annual internal review of their information security practices and physical security measures, including a risk assessment (if required).

Respond to information security incidents and breaches

A security incident or breach is when an ICT business system, facility or asset is accessed by an unauthorised party. This may include inappropriate access to, release, or loss of SENSITIVE or PROTECTED information. Examples include:

- an external attacker compromises the department's network to access employee records
- the loss or theft of departmental materials containing SENSITIVE or PROTECTED information, such as paper documents, laptops or portable storage devices
- a student opens an email enabling ransomware to lock a school or departmentally provided computer
- an employee accesses a student's records without a legitimate business reason.

Employees must report suspected or discovered information security incidents and/or breaches as soon as possible to their supervisors, managers, principals, directors or above and:

- isolate any device infected, or suspected to be infected, by malware or other suspicious software, by disconnecting it from any docks, hubs or network cables and turning off Wi-Fi
- submit an Information security incident (DoE employees only) Services Catalogue Online (SCO) form or contact the IT Service Centre on 1800 680 445
- report incidents related to:
  - a privacy data 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

- a breach of cardholder data to the Corporate card team using the Corporate card enquiry form (DoE employees only) and/or Integrity and Employee Relations Unit in accordance with the Corporate card procedure
- violations of the Queensland Government's Code of conduct for the Queensland public service and department's Standard of practice to the Integrity and Employee Relations Unit.

Definitions

Term	Definition
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.
Encryption	Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
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 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 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,

Term	Definition
	extranet, email, instant messaging, artificial intelligence (AI) including generative AI, 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.
Information security	Information security is the preservation of confidentiality, integrity and availability of information, in addition to other properties such as authenticity, accountability, non-repudiation and reliability.
Information security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of an ICT business system or the information stored, processed or communicated by an ICT business system.
Malware and malicious code	Any code or software that brings harm to an ICT business system, or is used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malwares include Trojans, viruses and worms.
Mobile device	A portable 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.
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.
Privacy data breach	A privacy data breach or potential breach may include an action or omission that results in loss, theft, misuse or unauthorised disclosure or use of personal information. A privacy data breach occurs if the department does not deal with a person's personal information in accordance with its obligations under the *Information Privacy Act 2009* (Qld) and associated Queensland Privacy Principles.

Legislation

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

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Information management, privacy and security policy

Other resources

- Information security guideline (DoE employees only)
- Code of Conduct for the Queensland Public Service and department's Standard of practice
- Corporate card procedure
- Enterprise risk management (DoE employees only) OnePortal page
- ICT asset management procedure
- Information classification and handling guideline (DoE employees only)
- Information security classification (DoE employees only) OnePortal page
- iSecurity (DoE employees only) website
- Privacy data breach and complaints procedure
- Procurement and purchasing procedure
- Queensland Government's Information and cyber security policy (IS18)
- Use of ICT services, facilities and devices guideline
- Use of mobile devices procedure

Contact

For general information security classification enquiries, please contact:

Enterprise Information Services, Governance Cyber and Policy, Digital Innovation Division
Web: Records management enquiry (DoE employees only)

To report an incident or request support, please contact:

Information Security Services, Governance Cyber and Policy, Digital Innovation Division
Web: Report security incidents (DoE employees only)

For more information about privacy data breaches, please contact:

Privacy, Privacy and Safer Technologies, Digital Innovation Division
Email: privacy@qed.qld.gov.au

For procedure or standards information, please contact:

Governance Risk and Compliance, Governance Cyber and Policy, 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 Information security procedure

Creative Commons licence