Information management, privacy and security policy

Version: 1.0 | **Version effective**: 01/07/2025

Audience

Department-wide

Purpose

This policy outlines the Department of Education's (the department) approach to information management, privacy and security, including the collection, storage, use, transfer, disclosure and protection of personal information and information assets, such as records and data.

Policy statement

A comprehensive and effective approach to the management of information, privacy and security is vital to empowering the department and its staff to make good decisions, manage risk, maintain privacy and confidentiality, and act compatibly with human rights.

The department's commitment to effective information management enables information to be managed consistently, appropriately and accurately to add value to business operations, and achieve departmental objectives. Information is managed as a valuable asset that informs decision making and it is governed and secured accordingly throughout its life.

The department is committed to safeguarding the privacy of individuals through the protection of personal information which it holds. Personal information is collected, stored, used, transferred and disclosed responsibly and in compliance with legislative obligations.

The department is committed to the security of its services and information. A consistent, risk-based approach to the implementation of information and cyber security helps the department to maintain confidentiality, integrity and availability, and prevent and effectively respond to security incidents.

Principles

Principle	What this means for the department
Information governance	• Strong governance arrangements support risk management activities for the department's information management and security. • Departmental records are managed using a lifecycle approach that holistically considers planning, sourcing, storage, use, assessment, disclosure and disposal of information. • Information is properly stored, accurate, reliable and protected from accidental or unauthorised modification or disposal.
Privacy	• The department only collects the personal information it needs to perform its functions. When individuals are asked to provide personal information to the department, they are told what is being collected, how it will be used, stored and disclosed, and if it will be transferred outside of Australia. • Personal information, including in relation to transferring personal information outside Australia and contracted service providers, is managed and protected from unauthorised access, use, disclosure and loss. • The department only uses personal information for the purpose it was obtained for and only allows access to employees who need it to perform their duties. • Privacy data breaches and complaints are managed in a timely and fair manner and in accordance with statutory obligations.
Information security	• Managed through a continuous risk-based approach including regular reviews and updates to procedures, processes, ICT standards, and training materials to reduce the likelihood and consequences of security breaches. • Departmental information is consistently classified using an established information security classification approach, ensuring it is only available to those who need it. • Robust processes are in place in schools, regional, and central offices to manage and monitor access to and use of departmental systems, and to protect personal information and maintain privacy. • Data breaches and unauthorised access to information can be swiftly identified, responded to and notified (as required).
Accountability, transparency and improvement	• Employees understand their ethical and legal obligations when accessing and using departmental systems and information. • Reporting assurance and attestation activities offer insights into areas of strength and compliance, and opportunities for improvement.

Principle	What this means for the department
	• Employees will be kept up-to-date with changes to information management requirements through departmental communication channels, updates to procedures, ICT standards and training. • All staff understand copyright and intellectual property requirements and do not infringe the rights of owners of third-party materials.
Access and use	• The department proactively provides the community access to appropriate information quickly and at a low cost. • Data and information can readily be provided to the right people for the right purpose at the right time. • Departmental systems and services are reliable and available for staff and customers when needed. • All staff only access systems when they have a legitimate reason to do so. • All staff only release, share or access information (including personal information) when they are authorised to do so.

Requirements

The department adheres to the Queensland Government Enterprise Architecture (QGEA) as part of the *Financial Performance Management Standard 2019* (Qld). Through this policy, the department aligns to key aspects of the QGEA as they relate to information management, privacy and security. This helps to achieve a cohesive and standardised approach to information management and security across the public sector.

Information management

The department's approach to information management aligns with the Queensland Government's Information asset custodianship policy (IS44), Information governance policy and Information access and use policy (IS33).

Information governance

The department's policies, systems and reporting practices ensure information is managed with the highest level of integrity and accountability. The department assigns clear roles and responsibilities to employees for the governance of information, making decisions around information management open and traceable. Increased transparency allows the public to see how their information is being handled and gives them confidence it is being ethically managed and appropriately used.

Managing information assets

Information is treated as an asset throughout its life which includes creation/collection, storage, use, disclosure/release, and disposal of information by the department and its employees, as well as information governance. The department identifies its information assets and assigns them to an information asset custodian who ensures their asset is managed throughout its life.

The department maintains an information asset register to record the existence of information assets, identify information asset custodians, document classifications and licenses, storage, and permitted usage of each information asset.

Records management

The *Public Records Act 2023* (Qld) requires the department to make and keep full and accurate records of its activities in accordance with the Queensland Government's Records governance policy. The department will create and maintain records to ensure actions or decisions are documented and can be referred to when needed.

Employees respectfully and securely handle the records in their care. They understand their obligations under relevant departmental procedures, legislation and guidelines including Code of Conduct for the Queensland Public Service and the department's Standard of practice and undertake annual training on their obligations.

Information access and use

Access to government information is a human right and a fundamental part of an open and transparent government. The public and department employees have a right to access the information that the department holds. The Administrative access to information procedure supports the department to meet its obligations under the *Right to Information Act 2009* (Qld), *Information Privacy Act 2009* (Qld) and Queensland Government's Information access and use policy (IS33) by establishing clear processes for requesting and releasing departmental information.

Administrative access supports the department's proactive approach of providing the public with quick and low-cost access to appropriate information. Where this release is not appropriate, the department manages formal applications under the *Right to Information Act 2009* (Qld) (RTI Act).

Intellectual property and copyright

Intellectual property, including copyright, is appropriately identified and used to ensure compliance with legislation, regulatory and contractual requirements.

The department's Copyright and other intellectual property procedure assists staff in meeting their obligations under the *Copyright Act 1968* (Cth) and the Queensland Government's Information access and use policy (IS33).

When the department uses third-party copyright materials it gets appropriate permission, follows licence requirements, attributes the materials correctly, and respects the rights of moral rights owners, and copyright owners and creators. State owned copyright materials published by employees for the department are covered by the appropriate copyright statement.

Consideration is given to Indigenous Cultural and Intellectual Property Rights when the department is managing or developing content which includes contributions from Aboriginal peoples and Torres Strait Islander peoples.

Privacy

This policy outlines how the department manages personal information in relation to its functions, requirements and activities. It supports the department's obligation to comply with the *Information Privacy Act 2009* (Qld) (IP Act), including the Queensland Privacy Principles (QPP), and the RTI Act. The department and its employees also recognise, consider and act compatibly with the right to privacy under the *Human Rights Act 2019* (Qld).

Collection of personal information

'Personal information' as defined in the IP Act is summarised as information or an opinion about an identified individual or an individual who is reasonably identifiable - whether true or not, and whether recorded in a material form or not.

The department only collects the personal information it needs to perform its functions. The department collects personal information directly from individuals, or in the case of students, from their parents/carers. When individuals are asked to provide personal and sensitive information, they are told what is being collected, how it will be used, stored, and disclosed. Personal information is collected directly from people who access the department's services and indirectly from third parties as part of carrying out its functions. These functions include the provision of an early childhood and education system.

The department may also collect sensitive information (for example health information, criminal record, religious belief, ethnic origin, union membership) and will generally only collect it directly from the individual it is about (or in the case of a student, their parent/carer), or otherwise with our obligations under the IP Act.

The following list gives examples of personal and sensitive information commonly collected and held by the department and is not exhaustive:

- name, address, phone number or personal email addresses of students, parents or guardians, employees and other stakeholders
- photographs of an employee or student
- bank account or financial details of employees, students, parents or guardians
- details of a student's education history or learning difficulties
- details of an employee's education or education activities
- allegations against an employee or details of offences they may have committed
- information received as part of, or collected as a result of, complaints made to the department
- information gathered during pre-employment interviews, reference checks and testing
- sensitive information including:
    - medical details or health information of employees and students
    - a parent or guardian's marital status, employment details, court orders or domestic violence records.

Use and disclosure of personal information

The department only uses and discloses personal information for its collected purposes. Personal information will not be disclosed outside of the department except under circumstances permitted by the IP Act including:

- if the person has given consent for its disclosure
- to stop or hinder a serious threat to an individual or the public
- if it is legally required or authorised
- if it is reasonably needed to assist a law enforcement agency.

Access and correction of personal information

Under the RTI Act people have a right to access and correct their personal information held by the department. The department informs people of:

- what kinds of personal information it holds and why
- how to access personal information
- how to amend information if they believe it is not accurate.

The department takes steps to ensure personal information is accurate, complete, up-to-date, and relevant prior to using it. When ensuring information accuracy, the department considers several factors including:

- the nature and sensitivity of the information
- how long ago the information was collected
- how quickly the information may become outdated
- who provides the information
- what the information is used for
- the consequences for people if their data is not accurate, complete and up-to-date.

When deciding if personal information is appropriate to use, the department will consider:

- how the personal information will be used
- if the personal information is directly related to that use
- what the department is trying to achieve when it uses the information
- any legislation or policies that relate to or govern that use.

Disclosure out of Australia

The department may be required to transfer an individual's personal information to an entity outside Australia, for example if:

- the department uses a cloud provider with servers located outside of Australia
- students use a non-departmental web service hosted outside Australia
- a school provides an international secondary student exchange program
- a school provides a course to students located overseas.

When collecting personal information, the department will inform individuals if their information will be disclosed overseas, why it will be disclosed and to which country. Personal information collected by the department can only be transferred to an entity outside of Australia if:

- it meets the circumstances permitted by the IP Act in the above section 'Use and disclosure of personal information' or
- two or more of the following apply:
    - the recipient of the personal information must handle personal information in relation to a law, scheme or contract that is substantially like the QPPs

  - the department has taken reasonable steps to ensure the recipient will not hold, use, or disclose the personal information in a way that goes against the QPPs
  - the department needs to transfer an individual's personal information to carry out its functions, related to them
  - the transfer benefits the individual, but it's not practical to ask for their agreement; however, if it were practical, they would likely agree.

Privacy complaints

The department manages privacy complaints in an accountable, transparent, timely and fair manner. The Information privacy breach and privacy complaints procedure outlines the department's process for managing privacy complaints.

A privacy complaint may also be a human rights complaint as section 25 of the Human Rights Act 2019 (Qld) protects a person's right to privacy.

Individuals can only make a privacy complaint about their own personal information, or on behalf of a student in their care, about an act or practice of the department in relation to their personal information and must:

- provide the privacy complaint in writing to a departmental employee
- state an address to which the department may respond to the complaint
- give particulars of the act or practice that is the subject of the complaint
- make the complaint within 12 months after the complainant became aware of the act or practice that is the subject of the complaint.

Privacy complaints can be emailed directly to the department's privacy team at privacy@qed.qld.gov.au or sent by post to Privacy Officer, Department of Education, PO Box 15033, City East Qld 4002.

A privacy complaint can also be submitted in writing through the customer complaints process. These complaints are referred to the department's Privacy team to progress on behalf of the department. Privacy complaints received by schools, regional offices and central office (in any written format, for example, email, post, electronic or physical) are also referred to the department's Privacy team to progress on behalf of the department.

The department has 45 business days to provide individuals with the outcome of their privacy complaint. The 45 business days start when the department received the compliant (for example, an email is received by a school or business unit).

If an individual is unsatisfied with the outcome received, or has not received one after 45 business days, they can refer the privacy complaint to the Office of the Information commissioner (OIC) for mediation.

If the OIC cannot resolve the complaint through mediation, the individual may choose to refer their privacy complaint to the Queensland Civil and Administrative Tribunal (QCAT). QCAT may make several orders after hearing a privacy complaint, including an award of financial compensation.

Information security

Information security management system

The department's information security approach meets the requirements of the Queensland Government's Information and cyber security policy (IS18).

Under this approach, the department's Information security management system (ISMS) is based on ISO/IEC 27001: Information security management systems. The ISMS provides the framework for the comprehensive protection of the department's information, application and technology assets by ensuring strong technical, physical and legal controls are in place so information risks can be effectively managed.

The ISMS aligns to the Enterprise risk management framework to ensure a systematic, consistent and cost-effective approach to risk management. Information security is an area of lowest risk appetite for the department and is managed as a priority.

The department allocates functions within the ISMS and clearly defines their roles and responsibilities. The Information Security Governance Committee provides strategic oversight and direction of information security activities in the department. This oversight helps escalate issues, identify trends, provide assurance and attestation activities, and strengthens the control environment for the information security enterprise risk.

Definitions

Term	Definition
Data	The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not information until it is utilised in a particular context for a particular purpose.
Data breach	A ‘data breach’ extends to any information held by the department and refers to: • unauthorised access to, or unauthorised disclosure of, the information • the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.
Eligible data breach	An ‘eligible data breach’ only involves personal information. For a data breach to be an ‘eligible data breach’ triggering notification and other obligations under the Mandatory Notification of Data Breach scheme, both of the following must apply: • there is unauthorised access to, or unauthorised disclosure of, personal information held by the department, or there is a loss of personal information held by the department in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

Term	Definition
	• the unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an ‘affected individual’).
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, head 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.
Information	Information is any data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. This includes presentation in digital, print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form. Information may also form a record or an information asset if it meets certain criteria.
Information asset custodian	The officer recognised as responsible for implementing and maintaining information assets according to the rules set by the owner to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility.
Information governance	Information governance is the system by which the current and future use of information and its management is directed and controlled.
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 management system (ISMS)	An ISMS is part of an overall management system (a type of framework), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
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

Term	Definition
Privacy complaint	A privacy complaint is a complaint by an individual about an act or practice of the department or an employee in relation to the individual’s personal information that is, or may be, a breach of the department’s obligations under the *Information Privacy Act 2009* (Qld) and associated Queensland Privacy Principles.
Sensitive information	Sensitive information includes: • information or an opinion about an individual's: o racial or ethnic origin o political opinions o membership of a political association o religious beliefs or affiliations o philosophical beliefs o membership of a professional or trade association o membership of a trade union o sexual orientation or practices o criminal records • health information about an individual, or • genetic information about an individual that is not otherwise health information, or • biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or • biometric templates.

Legislation

- *Copyright Act 1968* (Cth)
- *Education (General Provisions) Act 2006* (Qld)
- *Education (Queensland Curriculum and Assessment Authority) Act 2014* (Qld)
- Financial and Performance Management Standard 2019 (Qld)
- *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)
- *Right to Information Act 2009* (Qld)

- *Work Health and Safety Act 2011* (Qld)

Delegations/Authorisations

- Delegation of Director-General’s powers under Education (General Provisions) Act 2006 (Qld)
- Instrument of Authorisation - Powers, Functions, Authorities and Duties of the Public Authority and Executive Officer under Public Records Act 2002 (Qld)

Policies and procedures in this group

- Administrative access to information procedure
- Copyright and other intellectual property procedure
- Information asset and recordkeeping procedure
- Information security procedure

Supporting information for this policy

- Nil

Other resources

- Code of Conduct for the Queensland Public Service and Standard of practice
- Digital services policy
- Education and Training Sector Retention and Disposal Schedule
- Enterprise risk management framework
- General retention and disposal schedule (GRDS)
- ICT asset disaster recovery planning guideline
- ICT standards (DoE employees only)
- Information privacy breach and privacy complaints procedure
- Implementing information governance guideline
- Indigenous Cultural and Intellectual Property Protocol for the teaching of Aboriginal languages and Torres Strait Islander languages
- Information access and use policy (IS33)
- Information and cyber security policy (IS18)
- Information asset custodianship policy (IS44)
- Information asset register (DoE employees only)
- Information governance policy
- Information principles

- International Standard ISO 27001 - ISO/IEC 27001 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements (DoE employees only)
- Queensland public sector intellectual property principles factsheet
- Records governance policy

Contact

For further information about privacy, please contact:
Privacy team, Privacy and Safer Technologies
Email: privacy@qed.qld.gov.au

For further information on ICT policies, procedures and standards, please contact:
Governance Risk and Compliance, Information and Technologies Branch
Email: ICTpolicy@qed.qld.gov.au

Review date

1/07/2030

Superseded versions

Previous seven years shown. Minor version updates not included.

Nil

Creative Commons licence

Attribution CC BY

Refer to the Creative Commons Australia site for further information