Procedure

Records management procedure

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

Audience

Department-wide

Purpose

This procedure outlines the process for identifying, managing, using and disposing of Department of Education's (the department) records.

Overview

A record is information in digital or physical form that provides evidence that a business transaction has taken place or a decision has been made. Every employee is responsible for managing the records they create or receive during their employment. Employees must identify, capture, secure, store, use, share and dispose of records appropriately.

Records include anything on which there is writing or marks, figures or symbols that have a meaning, or from which sounds, images or writings can be reproduced. Records come in many formats, including:

- digital or electronic (digital) records such as emails and their attachments, word documents, texts, web pages, social media or online system content, data logs and tables
- physical records such as paper, film, printed photos, books, bound ledgers or registers.

Records do not include information that does not provide evidence of a business activity, transaction or decision such as a phone list, personal email that does not discuss any business activities, an exact copy of an existing record, messages received ‘for your information only’, calendar invites, meeting reminders or room bookings etc. These are known as transitory or ephemeral records. No approval process is required to dispose of these records.

This procedure supports the department's systematic and effective creation and management of complete and reliable records in accordance with the *Public Records Act 2023* (Qld) and Queensland State Archives (QSA) requirements.

This procedure is supported by the Information management, privacy and security policy, the Records management OnePortal pages (DoE employees only) and the Queensland Government’s Records governance policy.

Responsibilities

All employees

- identify, create and manage records
- protect records in accordance with each record's information security classification (see Information security classification OnePortal page) (DoE employees only)
- access records only when necessary to perform the duties of their role
- save all records received or created into an authorised recordkeeping system as soon as practicable
- ensure records created or received in a digital format remain in a digital format wherever possible
- undertake records management training such as provided in the yearly mandatory training programs
- take reasonable precautions to protect all records against unauthorised or illegal access, use, disclosure, modification or duplication, deletion or disposal.

Employees with additional recordkeeping duties

- ensure records are captured, transferred and disposed of as outlined in the Records management OnePortal pages (DoE employees only)
- maintain records held offsite with a secondary storage provider (DoE employees only)
- manage listings of all records for their school or business unit, both on and offsite, where records are not held within an authorised recordkeeping system
- liaise with the Enterprise Information Services (EIS) unit to transfer records to QSA
- process the Damaged records notification form (DoE employees only) in Services Catalogue Online if records have been damaged.

Managers, principals, directors and above

- oversee the records management activities for their school or business unit
- nominate an employee with additional recordkeeping duties in their school or business unit
- support and oversee employees with additional recordkeeping duties to undertake records management duties on behalf of the school, region or central office
- ensure appropriate records management processes are performed and key requirements are incorporated into local policies, procedures and subordinate work instructions
- secure information to prevent unauthorised access, amendment or disclosure
- liaise with the Enterprise Information Services unit when planning to upgrade, implement or decommission an application or ICT business system that holds records
- approve accounts and invoices with secondary storage providers.

Authorised responsible officers

- responsibilities are in accordance with the department's Instrument of Authorisation under the *Public Records Act 2002* (Qld).

Enterprise Information Services unit, Governance, Cyber and Policy, Digital Innovation Division (DID)

- advise on the management of records where required
- facilitate the transfer of permanent records to QSA
- assist in the salvage or disposal of damaged records.

Process

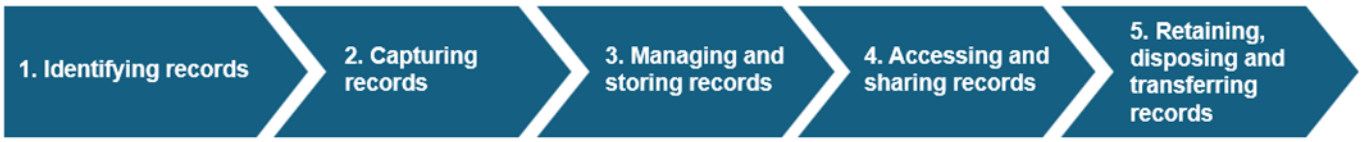

Image 1: Managing records in five key lifecycle steps

1. Identifying records

Employees must identify all records, digital (including those within social media or online services) and physical, created or received, in the course of performing their duties. Information should be captured as a record if it:

- signifies a change in policy, procedure or advice
- is required under legislation (for example, student admission register)
- requires a formal action such as signing or payment
- relates to the department's business activities (such as booking calendars for use of school property)
- documents advice given or received (for example, appeals of assessment results)
- documents a decision or action taken
- constitutes a high-value or high-risk record requiring special handling
- is an original document or a copy of an original document with additional notations (both are considered records).

If employees cannot determine whether information is a record, they must seek assistance from their manager, principal, director or above. Training is also available from OnePortal's Training sessions and webinars (DoE employees only) and Recordkeeping course (DoE employees only) within the Education Futures Institute.

2. Capturing records

Once a record has been identified, employees must:

- save or capture records within an authorised recordkeeping system to ensure the record can be managed:
  - regional and central office employees can manage digital records in Content Manager (see Authorised recordkeeping system definition below)
  - school staff can refer to the Storing digital files and information (DoE employees only) OnePortal page for a list of appropriate locations to store digital records

- apply naming conventions in accordance with Document naming conventions (DoE employees only) (KBA0034623)
- keep digital records in their original digital format, where possible
- save all departmental records received or created on privately-owned or department devices into an authorised recordkeeping system as soon as practicable
- label any records that are used in legal proceedings, appeals, court action, insurance claims, records protection notice, or are of cultural significance, if it is not obvious to the reader, as these are managed differently when reviewed for disposal
- use the Information security classification (DoE employees only) OnePortal page to assign an appropriate information security classification to the record
- apply the information security classification to the record as per the Information classification and handling guideline (DoE employees only).

Employees do not need to capture transitory or temporary records (such as those listed as 'Until business action completed' in the retention and disposal schedules) that no longer have a business use by deleting the digital records or using secure destruction bins for physical records. No approval process is required to dispose of these records.

Managers, principals, directors and above:

- must nominate an employee in their school or business unit to have additional recordkeeping duties and provide support, including training such as that provided through Education Futures Institute (DoE employees only)
- are responsible for providing employees with direction and support on the capture of records and departmental naming conventions (DoE employees only) (KBA0034623)
- must liaise with the Enterprise Information Services unit when upgrading, implementing or decommissioning any application or ICT business system that holds records.

Employees with additional recordkeeping duties:

- assist employees to properly store records as outlined in the Records management (DoE employees only) OnePortal page
- assist employees to secure records based on their information security classification and store them in appropriate locations
- determine how long records need to be kept for (DoE employees only) and if they are temporary or permanent (DoE employees only).

For further information about capturing records refer to the Records management (DoE employees only) OnePortal pages.

3. Managing and storing records

Employees must actively manage and store records and:

- keep records updated so they are adequate, complete and accurate

- store records in accordance with the Information security classification and handling guideline (DoE employees only) and, if required, return records to their secure storage location after use
- properly handle records with a security classification of SENSITIVE or PROTECTED and never leave them unattended in an unsecured area, such as open on a computer or left on an employee's desk (refer to the Information security procedure for more information)
- ensure a record's information security classification is not changed when the record is transferred to another location.

Employees with additional recordkeeping duties must:

- if physical records are stored onsite, ensure this meets the requirements of the Storing records onsite (DoE employees only) guideline
- transfer records that need to be kept long-term but are not in active use to a secondary storage provider
- seek a digital copy when requesting records from a secondary storage provider, where practical
- conduct yearly reviews of records held in secondary storage providers and on premises and, determine if they are past their retention time.

Managers, principals, directors and above must:

- oversee the management of their school's or business unit's listing of all records
- coordinate the batch scanning (digitising) of records by following Digitising physical records (DoE employees only) OnePortal page.

For further information about managing and storing records refer to the Records management OnePortal pages (DoE employees only).

4. Accessing and sharing records

Employees must only access records they need to perform the duties of their role.

When using or sharing records, employees must consider whether the person requesting access needs the record to undertake their role.

Managers, principals, directors and above must approve requests made by employees to access the records they need to perform the official duties of their role.

5. Retaining, disposing and transferring records

Records that have reached the end of their minimum retention time, as per the retention and disposal schedules (DoE employees only), can be transferred to QSA if listed as permanent in the relevant retention or disposal schedule, or temporary records destroyed through an approved transfer or destruction process. Permanent records must not be destroyed.

If a record exists in both a physical and digital form, both formats must be destroyed at the same time. Approved methods of destroying digital records are outlined in the Confirm records for disposal, storage or transfer OnePortal page (DoE employees only).

At least annually, employees with additional recordkeeping duties must:

- review records for destruction to confirm:
  - retention time has not changed using a current retention and disposal schedule
  - retention time has expired
  - records are not required for ongoing legal proceedings, appeals, court action, insurance claims or records protection notice
  - records do not need to be kept for ongoing business needs
  - records do not have any cultural significance
- if records are to be disposed of, seek approval from the authorised responsible officer to dispose of the records (DoE employees only) (KBA0034616)
- seek Enterprise Information Services unit advice to transfer permanent records to QSA including completing QSA's application forms as described in Confirm records for disposal, storage or transfer (DoE employees only).

Employees with additional recordkeeping duties must also undertake the following tasks when required:

- salvage, where possible, damaged records by following the How to handle damaged records (DoE employees only) (KBA0034451)
- must notify the Enterprise Information Services unit if the school, regional or central office has records of a permanent value, or that are more than 25 years old, and are at risk of loss or damage
- liaise with the Enterprise Information Services unit for additional support in managing the disposal of the damaged or lost records, including completing the Damaged or lost records notification form (DoE employees only) in Services Catalogue Online
- must arrange the destruction of the physical records using a secondary storage provider (DoE employees only), following approval from the authorised responsible officer. Including requesting a certificate of destruction as evidence of the destruction and, if necessary, arrange for the digital/electronic records to be destroyed.

Managers, principals, directors and above are responsible for overseeing the records management activities for their school or business unit.

For further information about retention and disposal of records refer to the Records management OnePortal pages (DoE employees only).

Definitions

Term	Definition
Authorised recordkeeping system	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 records management requirements such as *Public Records*

Term	Definition
	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. 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 under Records management (DoE employees only) in OnePortal.
Authorised responsible officer	An authorised responsible officer is a person holding a position authorised by the Director-General under the Instrument of Authorisation under the *Public Records Act 2002* (Qld) to approve the destruction of records, set and change restricted access periods, approve access to restricted departmental records including those held by Queensland State Archives, and approve the destruction of original paper records after digitisation (scanning). Authorised responsible officers include principals, Executive Director, Governance Cyber and Policy, Assistant Director-General's Digital Innovation and the Deputy Director-General, Digital Innovation.
Capture	A deliberate action which results in the registration of a record into an authorised recordkeeping system.
Digital records	Records created, communicated and/or maintained by means of electronic or computer equipment including both digital by design records and records that have been digitised.
Digitising	The process of converting a physical record to a digital representation. This may be done by such means as scanning or digital photography.
Disposal	Disposal of a record, includes destroying or damaging the record (or part of it) or altering, deleting, abandoning, transferring, donating, giving away or selling the record (or part of it).
Records protection notice	A directive issued by the Director-General or the Queensland State Archives that stops, for any length of time, the destruction of records relating to a specific topic or event.
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

Term	Definition
	should have regard for this procedure.
Employees with additional recordkeeping duties	Employees with the responsibility to manage records of their school or business unit as appointed by their manager, principal, director or above. This may include the management of digital records and back-up tapes or the archiving of physical records. This could be a Business Manager or their team member in a school or an Executive Support Officer role in a regional or corporate office.
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.
Permanent records	Records of permanent value as defined in Queensland State Archive's retention and disposals schedules.
Physical record	A physical record is a record not captured in a digital format. It may include records such as ledgers, registers, papers, photographs and films made with light-sensitive media, video tapes, phonograph records and older magnetic sound recordings.
Record	A record is information created or received by the department that provides evidence of a business transaction, the conduct of affairs or a decision being made. A record takes many forms including writing, marks, figures, symbols or anything from which sounds, images or writings can be reproduced or a map, plan, drawing or photograph. It can be in a digital, electronic or physical form.
Secondary storage provider	A company that provides a storage area where records can be stored prior to disposal through destruction or transfer to Queensland State Archives.
Social media	Social media records can include posts, comments, likes, tweets, retweets in tools such as Facebook, Flickr, X (formerly Twitter), Yammer and YouTube that provides evidence of a business transaction, the conduct of affairs or a decision being made which includes the original post and comments. Records can be captured through paid services, built-in export tools, print screen function or using a ‘save as’ or ‘save page as’ function.
Transitory or temporary records	Items of short-term value that are not required to be kept as records otherwise known as ephemeral information. This information is generally created as part of routine transactional business practices such as messages received ‘for your information only’, calendar invites, meeting reminders or room bookings, and are not required for ongoing business. No approval process is required to dispose of these records.

Legislation

- *Information Privacy Act 2009* (Qld)

- *Public Records Act 2023* (Qld)
- *Right to Information Act 2009* (Qld)

Delegations/Authorisations

- 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

- Copyright procedure
- Privacy data breach and complaints procedure
- Information management, privacy and security policy

Supporting information for this procedure

- Nil

Other resources

Department of Education

- Document naming conversations (DoE employees only) (KBA0034623)
- FAQ – Intro to Records Management (DoE employees only) (KBA0032885)
- ICT standards (DoE employees only)
- Information classification and handling guideline (DoE employees only)
- Recordkeeping course (DoE employees only)
- Recordkeeping training and resources (DoE employees only)
- Records management's OnePortal pages (DoE employees only)
- Storing digital information (DoE employees only)

Queensland Government

- Mandatory standards for records management
- Records governance policy
- Records storage, retrieval and destruction services standard offer arrangement
- Restricted access period (RAP) notice
- Transfer proposal form
- Transitory and short-term public records

Contact

For Content Manager support contact:
Records Support team, IT Service Centre
Digital Innovation Division
Form: Services Catalogue Online (SCO) (DoE employees only)

For information management advice contact:
Enterprise Information Services unit
Digital Innovation Division
Email: Service Catalogue Online (SCO)

For further information on ICT policies, procedures and standards, 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.

1.0 Information asset and recordkeeping

Creative Commons licence

Attribution CC BY

Refer to the Creative Commons Australia site for further information