Procedure

Information asset and recordkeeping

Version effective: 07/02/2020
Version: 1.2

Audience

Department-wide

Purpose

Provide the requirements for managing the department's information throughout its lifecycle including data, information assets and records.

Provide the requirements for recordkeeping practices within the department to meet legislative obligations.

Overview

The department is required under the Queensland Government's Information asset custodianship policy (IS44) to identify and register information assets and assign roles and responsibilities to information assets, to protect information in accordance with Information security policy (IS18:2018), to make full and accurate records in accordance with the Records governance policy and lawfully dispose records in accordance with the Records governance policy.

The department is required under the *Public Records Act 2002* (Qld), *Financial Accountability Act 2009* (Qld), *Financial and Performance Management Standard 2019* (Qld) and other legislation and administrative requirements to keep and maintain records of the department's activities.

Responsibilities

Director-General

- is accountable for information management and recordkeeping activities of the department
- has authority to delegate 'responsible officers' for the disposal of business records under *Public Records Act 2002* (Qld)
- has authority to delegate 'authorised officers' to set and change restricted access periods and approve access to restricted records under the *Public Records Act 2002* (Qld)
- holds authority for the disposal of original paper records after digitisation.

Deputy Director-General, Corporate Services

- has delegation as an 'authorised officer' to set and change restricted access periods and approve access to restricted records, including those held by Queensland State Archives, under the *Public Records Act 2002* (Qld)
- has delegations as a 'responsible officer' to authorise the disposal of business records (except the disposal of original paper records after digitisation which requires Director-General approval).

Information custodians - Assistant Director-Generals and nominated executive directors

Information custodians are accountable for the overall management of information, maintaining its relevance and ensuring that information under their control can be found, used and disseminated appropriately. Accountabilities include:

- ensuring information products are sourced to meet strategic needs
- ensuring the accuracy of conceptual information maps and data flow diagrams
- ensuring acceptable level/standard of information quality is defined
- determining when an information product is no longer required to be collected, stored and/or retained.

Other responsibilities:

- authorising appropriate methods of data collection and sourcing
- approving an appropriate information security classification and applicable privacy considerations (for a list of pre-approved classifications, refer to the Information asset register (DoE employees only))
- authorising the storage of any information products.

For a list of information custodians and the information within their control, refer to the Information asset register (DoE employees only).

Assistant Director-General, Information and Technologies

- has delegation as a 'responsible officer' by the Director-General under the *Public Records Act 2002* (Qld) to authorise the disposal of business records (except the disposal of original paper records after digitisation which requires Director-General approval)
- has delegation as an 'authorised officer' to set and change restricted access periods and approve access to restricted records, including those held by Queensland State Archives, under the *Public Records Act 2002* (Qld).

Employees

All employees are responsible for managing the safe transport, storage of and access to departmental information. This includes:

- managing all information (physical and electronic) in a manner consistent with its approved information security classification (for a list of pre-approved classifications, refer to the department's Information asset register (DoE employees only)
- managing records (received or created) that provide evidence of the business of the department including capturing information required to be created or kept under statutory legislation with financial or legal implications and which may come under scrutiny

- capturing and maintaining all records within an authorised recordkeeping system to maintain them. For corporate users, the department's authorised recordkeeping system is HP Record Manager. The department's email system and file hosting share drives (e.g. OneDrive) are not authorised recordkeeping systems
- takes reasonable precautions to protect all information against unauthorised access, illegal or unauthorised use, disclosure, modification, duplication, disruption and/or destruction
- ensuring that requests and the handling of departmental records containing personal information are managed in accordance with the Information privacy and right to information procedure
- making sure any intellectual property including copyright is appropriately identified, labelled and registered in accordance with the Intellectual property and copyright use procedure
- ensuring records are retained and disposed of following the department's Records retention and disposal handbook (DoE employees only) and that any disposals are authorised by a 'responsible officer' as outlined in this procedure
- completing the Keys to managing information (DoE employees only) online training course upon induction to the department and as a subsequent refresher training program on an annual basis. This applies to all corporate staff and specific school-based roles (please refer to the Mandatory annual training ready reckoner: 2020 edition).

Managers, directors, principals and above

- manages approvals to access and use departmental information within the bounds of approval granted by the information custodian
- ensures appropriate information management and recordkeeping processes and training within their business unit or school, including through encouraging staff to undertake the Keys to managing information course refresher
- ensures the management of financial records is in accordance with applicable financial practices, including the Queensland Government Financial Management Practice Manual (FMPM) website (DoE employees only)
- secures information from unauthorised access, amendment or disclosure in accordance with the Information security classification and handling guideline
- ensures appropriate access controls are implemented and enforced such that classified or sensitive records are only available on a need-to-know basis
- ensures all records are retained as required for business, legislative, accountability and cultural needs in accordance with authorised retention and disposal schedules:
    - Queensland State Archives General Retention and Disposal Schedule (GRDS) (DoE employees only)
    - Early Childhood Education and Care Retention and Disposal Schedule (DoE employees only).

Principals or, executive directors or above

- have delegation as 'responsible officers' to dispose of business records in accordance with the department's Records retention and disposal handbook (DoE employees only) and in consultation with Director, Information and Governance Management. This excludes the disposal of original paper records

after digitisation which requires Director-General approval and consultation with the Director, Information and Governance Management

- in the case of schools, where a cloud-based solution will hold/holds departmental information, an information risk assessment must be performed (which can be found on Service Centre Online) considering:
    - any information risk assessment that results in an initial Low or Medium risk rating may be accepted by the principal
    - where the initial risk rating result is High or Extreme, the designated information custodian must be consulted and agree to accept the risk
    - should the information custodian not agree to accept the risk, the information cannot be held in the cloud-based solution.

Solution managers and 'information stewards'

Solution managers and 'information stewards' are responsible for the management of a specified ICT solution or service. In this role they must:

- implement and manage electronic processes to support the transfer/collection of sourced information in-line with legislative, regulatory and custodian requirements
- implement security controls commensurate with the approved information security classification and privacy restrictions
- implement data entry controls to support quality standards/requirements as outlined by the information custodian
- develop and maintain conceptual information maps and data flow diagrams
- ensure records that are generated as part of an ICT business system are captured and retained in accordance with the department's Records retention and disposal handbook (DoE employees only) within an authorised recordkeeping system
- liaise with the Director, Information and Governance Management for the migration of information from ICT business systems that do not have recordkeeping capability
- ensure records being held long term are retrievable in the format they have been captured in
- for Closed Circuit Television (CCTV) systems, maintain full and accurate records (i.e. adequate, complete, meaningful, authentic, secure, accessible, and usable) which must be kept according to the Queensland State Archives' Surveillance records requirements.

Director, Information and Governance Management, Digital Transformation, Information and Technologies Branch

- manages and maintains the department's information asset register
- manages, advises on and implement departmental records management activities including retention and disposal, digital continuity, authorised recordkeeping systems, training and other activities to ensure compliance with the *Public Records Act 2002* (Qld) and whole-of-government recordkeeping practices
- manages the processes to sentence and dispose of records in accordance with legislation
- sets standards for requirements of authorising systems to manage records

- provides advice to employees performing risk assessments and business needs analysis relating to the disposal of original hardcopy (paper) records after digitisation and seeking Director-General approval. Refer to the Queensland State Archives' Dispose of source records web page for further details.

Process

Information asset management

Information custodians and stewards must develop and implement processes to manage information assets throughout their lifecycle, including adherence to intellectual property, right to information and all other legislative and regulatory obligations. Administrative management processes include:

- reviewing the information asset annually, whether available publicly or internal to the department, to ensure it is relevant, accurate and that the quality and integrity is maintained
- updating and maintaining the information asset's metadata within the department's Information asset register (DoE employees only)
- reviewing and updating business continuity and disaster recovery plans regularly to reflect current processes, contacts and to ensure required equipment is readily available.

Hardcopy records management

Employees must manage hardcopy records in their care by:

- ensuring the hardcopy record is marked with an information security classification as per Information security classification and handling guideline
- ensuring requirements under the Intellectual property and copyright use procedure are complied with
- consulting with the Director, Information Management when undertaking digitisation of the hardcopy (original paper) record when required through scanning, ensuring compliance with the *Public Records Act 2002* (Qld) and other legislative requirements and seeking Director-General approval. This includes a risk assessment and business needs analysis, as not all hardcopy records can be destroyed following digitalisation. Refer to the Queensland State Archives' Dispose of source records web page for further details.

Electronic records management

Employees must manage electronic records in their care by:

- creating documents to include metadata such as date of creation, status, version, information security classification, purpose and contact (including business unit or school), if appropriate, to assist in any future release of documents
- creating or inputting data or information within an ICT business system or authorised recordkeeping system complete and/or review for currency and accuracy any required metadata
- inserting within the document's footer the information security classification as per Information security classification and handling guideline
- ensuring requirements under the Intellectual property and copyright use procedure are complied with

- storing or saving information in a central repository on the departmental corporate network and not saving local copies on device hard drives. Ensure (where it is not possible to centrally store records), records that are created and captured by mobile devices or removable media are transferred to an authorised recordkeeping system as soon as possible
- capturing the title and providing information about the record consistently to assist in later retrieval of the record, in accordance with the authorised recordkeeping system's required processes and the department's thesaurus:
  - Corporate Thesaurus – Introduction (DoE employees only)
  - Corporate Thesaurus – Terms (DoE employees only)
  - Business Classification Plan (DoE employees only) (a quick guide to controlled vocabulary used for classifying, titling and indexing records).

Definitions

Authorised officer	For this procedure, an officer who is delegated by the Director-General as an 'authorised officer' is authorised to set and change restricted access periods and approve access to restricted records under the *Public Records Act 2002* (Qld).
Authorised recordkeeping system	A system used to manage and provide access to records over time using a rigorous set of business rules intended to preserve the context, authenticity and integrity of the records. For corporate users, the department's authorised recordkeeping system is HP Record Manager.
Employee	Any permanent, temporary or seconded staff member, contractors and consultants, volunteers who assist staff with their professional duties, or other person who provides services on a paid or voluntary basis to the department that are required to comply with the department's policies and procedures.
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 custodian	An Information Custodian implements and maintains information assets and associated ICT resources according to the rules set in cooperation with the 'owner' to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility throughout its lifecycle. Custodian may be referred to as information custodian, data custodian or business system custodian or subject matter expert.
Information product	May be a dataset or an information artefact that has been compiled/created using data sourced from one or more points of origin.
Records	Records can be in hardcopy, electronic or any other form that provides evidence a business transaction has taken place or a decision has been made.
Responsible officer	For this procedure, an officer who is delegated by the Director-General as a 'responsible officer' is authorised to dispose of business records under the *Public Records Act 2002* (Qld).

Solution manager / information steward	A steward has the authority and accountability for ICT solutions or services that hold information assets, and approves the rules by which the solution/service is managed.

Legislation

- *Financial Accountability Act 2009* (Qld), part 4-5
- *Financial and Performance Management Standard 2019* (Qld)
- *Public Records Act 2002* (Qld)

Delegations/Authorisations

- Nil

Related policies

- Information Management (DoE employees only)
- Financial Management Practice Manual (FMPM) (DoE employees only)
- Queensland Government - Information asset custodianship policy (IS44)
- Queensland Government - Information security policy (IS18:2018)
- Queensland Government - Records governance policy

Related procedures

- Information privacy and right to information
- Intellectual property and copyright use
- Use of ICT systems
- CCTV use in schools

Guidelines

- Information security classification and handling guideline

Supporting information/websites

- Business Classification Plan (DoE employees only)
- Corporate Thesaurus – Introduction (DoE employees only)
- Corporate Thesaurus – Terms (DoE employees only)
- Queensland State Archives - Dispose of source records web page
- Queensland State Archives - Surveillance records web page
- Early Childhood Education and Care Retention and Disposal Schedule (DoE employees only)
- General Retention and Disposal Schedule (GRDS) (DoE employees only)
- Information asset register (DoE employees only)

- Keys to managing information (DoE employees only)
- Mandatory annual training ready reckoner: 2020 edition
- Records retention and disposal handbook (DoE employees only)

Contact

For further information, please contact:

- Information and Governance Management
  Information and Technologies Branch (I&T Branch)
  Email: InformationManagement.INFOMNGT@qed.qld.gov.au

Review date

01/11/2018

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 Information asset and recordkeeping
1.0 Information Management (IM)
4.0 Managing the department's records*
2.0 Providing access to departmental information*
3.0 Managing data held by the department*

* indicates procedures replaced by the Information Management procedure in 2014

Creative Commons Licence