Information Management (IM)

Version Number

1.3

Implementation Date

3/05/2017

Scope

Department-wide

Purpose

This procedure provides employees with their responsibilities to appropriately manage information (specifically records, data and information assets) which they may receive, create, use, store or dispose of within the department. This includes classifying information for appropriate protection and/or disclosure.

This procedure further enables the enhancement and integration of information management, empowers local decision making, and increases capability to share information between other government agencies and our partners.

Overview

This procedure has been divided into the following sections:

Responsibilities

Principals or, Executive Directors or above:

- are specifically delegated as 'responsible officers' by the Director-General under the *Public Records Act 2002* to authorise the disposal of business records
- designates a recordkeeping system as an 'authorised recordkeeping system' in compliance to Section 3 - Recordkeeping of this procedure.

Deputy Director-General, Corporate Services:

- has been authorised by the Director-General 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* except the disposal of original paper records after digitisation which requires approval by the Director-General.

Assistant Director-General, Information and Technologies:

- has been authorised by the Director-General 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* except the disposal of original paper records after digitisation which requires approval by the Director-General.

Director-General:

- is accountable for the recordkeeping activities of the department
- has authority to delegate 'responsible officers' for the disposal of business records under *Public Records Act 2002*
- 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*
- authorises the disposal of original paper records after digitisation.

Manager, Information Services, Information and Technologies Branch:

- is specifically delegated as 'responsible officer' by the Director-General under *Public Records Act 2002* to authorise the disposal of business records in accordance with the department's Records Retention and Disposal Handbook (DET employees only).

Process

1. Creation and use of information

Information in an **employee's** care such as documents, records, data and information assets must be managed appropriately including:

- inserting within the document or data (where possible) the information security classification as per Section 2 below
- recording information that is classed as a record (that is, any object that provides evidence of a business decision, transaction or activity or is received in the course of business) follows the recordkeeping requirements in Section 3 below
- identifying copyright work which is the result of original and creative effort undertaken by themselves and include within this work an appropriate Australian Governments Open Access and Licensing Framework (AusGOAL) creative commons licence (see Intellectual Property and Copyright Use procedure)
- when preparing information for publication (whether print or online, for public or internal websites) ensure that the department owns the copyright or, where applicable, has obtained specific consent of the copyright owner for publication
- when creating documents include metadata such as date of creation, status, version, purpose and contact (including business unit or school), if appropriate, to assist in any future release of documents
- when 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
- within emails adding a signature block (DET employees only) that contains name, position, business unit or school, contact phone number etc.

^ Top of page

2. Information security classification

Employees must apply an information security classification to information (e.g. draft document, record, spreadsheet) that they create process or handle according to different categories as outlined below to identify, protect and secure information when required:

- **Public**: Information authorised to be made publicly available, or able to be released to the public.

- **Unclassified**: Non-sensitive information that is created or received within the department, is used internally, and comprises the bulk of the information used within the department.
- **X-in-confidence**: Sensitive and confidential information that is created or received within the department. Access must be restricted to authorised persons on a 'need to know' basis. If released inappropriately, it might cause limited damage to the department or others.
- **Protected** (including Cabinet-in-confidence): Very sensitive and confidential information that, where unauthorised and/or premature disclosure might cause damage to one or more parties.
- **Highly protected**: Information that requires a substantial degree of protection as compromise of the information could cause serious damage to the state, the government, commercial entities or members of the public.

When managing this information **employees** that create, process or handle information must:

- ensure that electronic documents have their information security classification displayed on the front page, in a watermark, in the header or footer, in accompanying metadata, or document properties
- ensure that any changes to the classification applied that results in a lowering of the information security classification will be made through a formal approval process that involves the author and/or information custodian
- ensure that classification applied to an information item will not be changed whilst that item is being transferred to another location or between ICT business systems
- ensure information classified as X-in-confidence, protected or highly protected that is stored in mobile devices e.g. CDs, DVDs, USB devices, hard drives, SD cards is destroyed or not used for other purposes without being securely wiped or rendered unusable
- ensure that when using the information security classification it does not limit the legislation under which the department operates
- take reasonable precautions to protect information based on their information security classification against unauthorised access, illegal or unauthorised use, disclosure, modification, duplication, disruption and/or destruction.

For more information see the Information Security Classification and Handling Guideline.

^ Top of page

3. Recordkeeping

The department which includes its **employees** is required by the *Financial Accountability Act 2009*, *Public Records Act 2002*, and other legal and administrative requirements to keep and maintain proper records of the department's activities. The Director-General is accountable for the recordkeeping activities of the department.

Employees must manage records (whether received or created) which provides evidence of the business or affairs 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
- required as part of a report to internal or external bodies or where approval has been sought
- that identifies decisions which set a precedent, have impact on individuals or the department as a whole, or may need to be used as evidence
- that supports an existing record
- that identifies changes in policy, procedure or methodology
- that is of interest or importance outside of the immediate work environment
- is of a business, administrative or historical value.

These records are to be captured regardless of technology being used and could be in a physical (e.g. paper), electronic (e.g. email, text message) or object form (e.g. video and audio).

^ Top of page

When capturing, creating, managing or disposing of records **employees** must:

- capture and maintain all records within an authorised recordkeeping system
- ensure where records are created and captured by mobile devices (laptops, tablets, phones, USB's etc.) that these records (email, text or instant messages, documents etc.) are transferred to an authorised recordkeeping system as soon as possible. Employees must ensure the date and time of the transaction and all the stakeholders involved are evident when capturing the record. The records can be transferred by forwarding them directly to the employee's work email or transferred via USB or other device
- capture, title and provide 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 (DET employees only)
  - Corporate Thesaurus – Terms (DET employees only)
  - Business Classification Plan (DET employees only)(a quick guide to controlled vocabulary used for classifying, titling and indexing records)
- undertake any digitisation of a record through scanning, ensuring compliance with the *Public Records Act 2002* and other legislative requirements. This includes a risk assessment and business needs analysis, as not all records can be destroyed following digitalisation. Disposal of original paper records after digitisation requires consultation with the **Manager, Information Services, Information and Technologies Branch** and approval by the **Director-General**. See the Queensland State Archives' Digitise and dispose of records web page for further details
- take reasonable precautions to protect records and authorised recordkeeping systems against unauthorised access, illegal or unauthorised use, disclosure, modification, duplication, disruption and/or destruction
- apply security access controls for records according to their information security classification; managing, protecting, labelling, handling and storing the record according to the Information Security Classification and Handling Guideline
- ensure that requests and the handling of departmental records containing personal information are managed in accordance with this procedure's Section 4 - Personal information
- ensure records are retained and disposed of following the department's Records Retention and Disposal Handbook (DET employees only) and that any disposals are authorised by a 'responsible officer' delegated by the **Director-General**.

^ Top of page

Employees must complete those aspects of the Keys to managing information's (DET employees only) program specified in the Induction planner for their position. Employees can find further information on how to create and maintain records within the department's recordkeeping website (DET employees only).

Managers, directors, principals and above must ensure appropriate recordkeeping processes and training within their business unit or school and:

- ensure the management of financial records is in accordance with applicable financial practices such as the Financial Practices in Schools and other Education Centres Procedure
- approve access and secure records from unauthorised access, amendment or disclosure in accordance with the information security classification and authorised recordkeeping system
- ensure 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 for Administrative Records (GRDS)
  - DET Retention and Disposal Schedule for Education Records (DET employees only)

- DET Retention and Disposal Schedule for Early Childhood Education and Care Records
- DET Retention and Disposal Schedule for Vocational Education and Training Records (DET employees only).

Principals or, Executive Directors or above are specifically delegated as a 'responsible officer' by the Director-General, authorised to dispose of business records in accordance with the department's Records Retention and Disposal Handbook (DET employees only). This excludes the disposal of original paper records after digitisation which requires approval by the Director-General.

^ Top of page

Business system owner and/or information custodian accountable for a specified application or ICT business system must:

- ensure records that are generated as part of an ICT business system are captured and retained in accordance with the Records Retention and Disposal Handbook within an authorised recordkeeping system
- liaise with the Manager, Information Services for the migration of information from ICT business systems that do not have recordkeeping capability
- ensure records that have been captured can be retrieved if required in a range of media formats, e.g. hardcopy
- ensure generic requirements for recordkeeping functionality are included in authorised recordkeeping systems including a recordkeeping metadata scheme
- ensure any authorised recordkeeping system that links to or forms part of their ICT business system is reliable and secure, and appropriate to the generation, maintenance and retrieval of records
- if the ICT business system is a surveillance and monitoring system implement full and accurate records (i.e. adequate, complete, meaningful, authentic, secure, accessible, and usable) according to Queensland State Archives' Surveillance records web page.

The **Manager, Information Services, Information and Technologies Branch** corporately manages, advises and implements recordkeeping activities including retention and disposal, digital continuity, document and file management, recordkeeping systems, disaster preparedness and recovery plans, education and training. The role further has responsibility to:

- as a 'responsible officer' specifically delegated by the **Director-General**, this role is authorised to dispose of business records in accordance with the department's Records Retention and Disposal Handbook (DET employees only)
- manage and develop the department's retention and disposal schedules, and seeks approval from the State Archivist
- undertake activities to ensure compliance with the *Public Records Act 2002* and whole of government recordkeeping policies.

^ Top of page

4. Personal information

Personal information is mainly protected under the Information Privacy Act 2009 which legislates how the department will:

- collect, store, use and disclose personal information about people (employees, students etc.)
- allow people access to their personal information held by the department
- allow people to request changes or amendments to this information.

Information Privacy Act 2009 applies to all personal information not covered by the department's primary legislation. This procedure and the Personal Information Guideline will assist **employees** to meet these legislative obligations and includes advice for schools.

Collection of personal information

Employees when collecting personal information must:

- only collect personal information directly from the individual, as required to carry out the tasks directly related to the functions and activities of the business unit or school
- only use departmental approved forms, questionnaires, interviews, survey tools or other tools used to collect personal information
- provide a privacy notice (see Personal Information Guideline – Attachment B) to the individual on collection of their personal information.

Security of personal information

Employees must apply protection to the personal information they control by:

- classifying personal information with an information security classification and applying security controls accordingly
- protecting and securing personal information in both paper and digital formats and on mobile devices from loss, unauthorised access, use, modification or disclosure, and any other misuse
- reporting any loss of personal information to their **Manager, Director or Principal**.

^ Top of page

Provision of personal information

The department publishes on its website details of the type of personal information it holds, for what purpose and use, which is maintained by the **Director, ICT Governance Strategy and Policy, Information and Technologies Branch**.

An individual whose information is held by the department has the right to expect that any access is permitted only for authorised purposes. **Employees** must:

- seek approval from their **Director, Principal or above** to undertake requests by individuals to access and amend their personal information
- when processing requests, undertake identity authentication to be satisfied as to the requestor's identity or the identity of the parent or guardian for an individual under 18 years, and their right to access or amend the personal information
- where there is doubt about an individual's right to access or amend personal information must advise them of the RTI and Information Privacy Application process.

Checking accuracy of personal information

Employees must check the accuracy, completeness and currency (i.e. up to date) of personal information before use.

Use and disclosure of personal information

Employees must only use personal information for the purpose for which it was collected, unless the individual concerned has consented to the use of the information for another purpose or an exception applies (see the Personal Information Guideline for details). Any approved use must be recorded in the individual's file or in the system where the personal information is stored.

Directors, Principals or above who authorise requests for disclosure of personal information must:

- ensure requests for disclosure of personal information are in writing and state why the information is required (see Obtaining and Managing Student and Individual Consent

Procedure)
- ensure the individual concerned is aware of, or has consented to that disclosure
- advise the recipient in writing to not use or disclose the personal information for a purpose other than the purpose for which it was provided
- ensure the disclosure:
  - is authorised by law to do so
  - is necessary for certain types of law enforcement
  - there are reasonable grounds in existence to indicate that the use of this information is necessary to prevent or lessen a serious and imminent threat to the life or health of that person
- record decisions to disclose (including reasons for disclosure and the information disclosed).

Principals are also to follow the Access to Records Held in Schools Procedure.

^ Top of page

Privacy complaints

Employees must direct any privacy complaints to the department's complaint directory website, except for schools which follow the Complaints Management – State Schools Procedure. The complainant will have a response within 45 business days.

The **Director, Ethical Standards** will manage the complaint referring it, if necessary, to the:

- Crime and Corruption Commission (CCC) as required under the *Crime and Misconduct Act 2001*, section 38, or
- Legal and Administrative Law Branch if a complaint proceeds to the Office of the Information Commissioner or Queensland Civil and Administrative Tribunal (QCAT).

In some instances it may be necessary for a matter to be referred back to the **Director, Ethical Standards** from the CCC for investigation in relation to a potential breach of the Queensland Government's Code of Conduct for the Queensland Public Service, the department's Standard of Practice and/or the *Public Service Act 2008*.

Privacy breaches

Any **employee** who suspects a breach of privacy must report it to their **supervisor, manager, director, principal** or directly using the complaint directory website. The **supervisor or manager** will assess the breach and/or consult with the **Director, Ethical Standards** to take necessary action.

^ Top of page

5. Information release, access and use

The department has a number of ways in which members of the community, employees, students and parents/guardians can access information held by the department. The department provides government information to the public to the maximum extent possible, unless on balance it is contrary to the public interest to do so.

Information held by a regional office or central office is also accessed in accordance with the Administrative Access Scheme for Central, Regional and District Offices process. Access to school related information follows Access to Records held in Schools Procedure. Employees can access their own records through the Human Resources Branch in accordance with the Public Service Regulation 2008.

Employees must be aware that any information held in the department (documents, data, emails, text messages, etc. including personal correspondence) can be made available and/or released to the public under *Right to Information Act 2009* (RTI) by:

- proactive publication to the website under 'published information' within specified categories of information (also known as a publication scheme)
- an administrative release where information is released to an individual or organisation at their request without having to lodge a formal RTI and Information Privacy Application
- a formal RTI and Information Privacy Application where the information and/or its metadata is published under the disclosure log on the department's website. Personal information requested under *Information Privacy Act 2009* also follows this process. This formal application for government-held information should only be made as a last resort.

^ Top of page

If an **employee** receives a request for information they must, in consultation with an **Information Access Officer** in their business unit, determine which process for release is to be followed considering:

- any requests for information from the media is directly forwarded to the **Community Engagement and Partnerships Branch** at media@det.qld.gov.au or to phone (07) 3237 1367
- request for the release of closed or restricted records including those held at Queensland State Archives is to be forwarded to the **Manager, Information Services**, Information and Technologies Branch as under the *Public Records Act 2002* they may require authorisation for release by the Deputy Director-General, Corporate Services or Assistant Director-General, Information and Technologies (who are authorised by the Director-General to set and change restricted access periods and approve access to restricted records)
- the information that is to be released complies with Section 1 - Creation and use of information section above
- the department support's the exchange of government information with other government entities where there is a business need and it is permitted or required by legislation
- if it has been determined the information can be released directly to the department's website under the publication scheme the Information Access Officer coordinates with **Web and Digital Production, Information and Technologies Branch** to release the information
- the Administrative Access Scheme (DET employees only) process must be followed for administrative releases
- the information must be provided to the maximum extent possible free of charge
- where unable to provide administrative release or a direct release to the department's website direct the requesting party to the department's website at: http://deta.qld.gov.au/right-to-information/make-a-request.html to make a formal RTI and/or Information Privacy Application.

^ Top of page

Employees when receiving a request for information requested under a RTI and Information Privacy Application are to:

- take all reasonable steps to locate relevant documents (both electronic or hardcopy documents) and respond by the due date set by the **Manager, Information Release**, Legal and Administrative Law Branch this includes:
  - any paper or other material on which there is writing
  - any paper or other material on which there are marks, figures, symbols or perforations having a meaning for a person qualified to interpret them, and
  - any disc, tape or other article or any material from which sounds, images, writings or messages are capable or being produced or reproduced (with or without the aid of another article or device)
- understand that if they do not provide all relevant documents the department and its officers may have to defend their conduct before the Information Commissioner or the Queensland Civil and Administrative Tribunal (QCAT). It could also result in an adverse report to Parliament about the department's non-compliance

- keep an accurate record of time spent searching for and retrieving the documents. However, the time spent by employees in photocopying or collating any materials or searching for documents where they should have been, but ultimately are not situated, cannot be recorded by the employee undertaking these tasks.

An **employee** who has been delegated the role of **Information Access Officer** for their business unit is to:

- provide advice on Right to Information and information privacy requests
- coordinate within the required timeframes approval processes including searching for the required information/documents consulting with **Legal and Administrative Law Branch**, when required
- prepare and advise on the administrative release of information following the Administrative Access Scheme (DET employees only) process
- create records where necessary within an authorised recordkeeping system of the original request and documents
- seek necessary approval according to the required process.

^ Top of page

Manager, director or above must:

- ensure information released on the Right to Information website meets the requirements of significance, accuracy and relevance
- approve the administrative release of information following the Administrative Access Scheme process
- coordinate regular reviews of information from, or about, the business unit on the department's Right to Information - published information website and other departmental websites to ensure the continued relevance, significance and accuracy of published information
- proactively identify new information for consideration to be published on the department's Right to Information website
- approve internet publication of all new and revised information ensuring it is accurate, relevant and has no copyright or other agreements restricting its release and publication
- ensure an Information Access Officer has been appointed to their business unit to adhere to this procedure.

^ Top of page

6. Information assets

Information owners and **custodians** must develop and implement processes to manage information assets through their lifecycle, including adherence to intellectual property, right to information and all other legislative and regulatory obligations including:

- identifying the information security classification/s of the information asset and based on such classification apply controls to manage, store, process or transmit the information assets
- providing access to information by employees based on sensitivity due to legislative, policy, standards, commercial or privacy reasons40
- processing, transferring or releasing information assets according to the handling practices listed in Information Security Classification and Handling Guideline
- maintaining created records in an authorised recordkeeping system , where appropriate
- incorporating a metadata scheme 43 where the information asset is an ICT business system
- making sure any intellectual property including copyright is appropriately identified and labelled40
- 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 being

maintained
- storing and maintaining information assets, including archiving and the undertaking of integrity checks of data, to ensure data has not been modified without authorisation or accidentally corrupted
- updating and maintaining the information asset's metadata within the department's information asset register (DET 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.

The business system owner is responsible for implementing appropriate security to protect the information asset from unauthorised access, use, disclosure, corruption or destruction in accordance with the Information and Communication Technology (ICT) procedure's identity (ID) and access management section.

An **information owner** is responsible for authorising processes for the transferral and disclosure of information from one system to another.

Director, ICT Governance Strategy Policy, Information and Technologies Branch is responsible for managing the department's information asset register.

Online Resources

Attachments

- Information Security Classification and Handling Guideline
- Personal Information Guideline
- Administrative Access Scheme for Central, Regional and District Offices

Supporting documents

- Queensland Government Chief Information Office policies and standards
- Code of Conduct for the Queensland Public Service

Online material

- Handling personal information podcast

Review Date

1/05/2014

Definitions

Authorised recordkeeping system
A system designed to capture, manage and provide access to records through time using a rigorous set of business rules which are intended to preserve the context, authenticity and integrity of the records. Authorisation is provided by a principal or, an executive director or above, ensuring the compliance of the recordkeeping requirements of this procedure.

Business system owner
Responsible for the maintenance, support and operation of the business system ensuring it is fit for purpose and meets the needs of information owners.

Digital continuity
The identification, appraisal, description, storage, preservation, management and retrieval of digital records, including all of the policies, guidelines and systems associated with those processes, so the logical and physical integrity of the records is securely maintained over time.

Employee
Any permanent, temporary, seconded or contracted 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. Within schools this includes principals, deputy principals, heads of departments, head of curriculums, guidance officers, teachers and other school staff who manage information.

ICT business system
Information technology systems or application designed to 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 equipment designed for a particular communication and/or function, including but not limited to computers, mobile devices, television sets, digital or analogue recorders including DVD and video, facsimile machines, photocopiers and, printers and other imaging equipment.

Information asset
Is 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. This includes transactional information in ICT business systems, documents and mail.

Information custodian
Delegated by the information owner to set and define the rules of an information asset to ensure the information asset is appropriately managed to maintain its currency, integrity and availability. This includes identifying its information security classification/s and, registering and maintaining its details within the department's Information Asset Register (DET employees only).

Information owner
The Director-General, Deputy Director-General or Assistant Director-General who approves the rules for the information asset and has authority and accountability for the collection and management of the information asset.

Mobile device
Is a type of ICT device and includes mobile and smart phones, 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. A voice only, or voice and data transmission, or data transmission only service may be purchased separately to the device. Data transmission provides internet access for web browsing and email.

School
Relates to Queensland State Schools including independent public schools.

Authority

- Queensland Government Chief Information Office policies and standards

Related Policy Instruments

- *Crime and Misconduct Act 2001* (Qld) Section 38
- *Financial Accountability Act 2009* (Qld)
- *Information Privacy Act 2009* (Qld) Chapter 2 Parts 1, 3 and 4; section 28, Chapter 3 to 6, Sch 1 -3

- *Public Records Act 2002* (Qld) Section 8(1), Division 2 and 3, Part 2
- *Public Service Act 2008* (Qld) Division 3 Functions S98, Ch 1, Part 3 and s154, Ch 5 Pt 4
- Public Service Regulation 2008 (Qld) Part 3 Section 14 and s10(2)(a-f)
- *Right to Information Act 2009* (Qld) Sections 21, 47, Chapters 1-7, Chapter 6 Part 1, Part 3
- Information Management (IM) policy (DET employees only)

Attachments

- Information Security Classification and Handling Guideline
- Personal Information Guideline
- Administrative Access Scheme for Central, Regional & District Offices

Contact

For assistance on releasing information to the department's websites contact:

- Web and Digital Production
  Log a job with Service Centre Online
  Call Service Centre on 1800 680 445 (press option 3, 3)
  Email: webworkrequest@det.qld.gov.au

Media enquiries are forwarded to:

- Community Engagement and Partnerships Branch
  Phone: (07) 3237 1367
  Email: media@det.qld.gov.au

For further support with TRIM:

- Log a job with Service Centre Online
  Call Service Centre 1800 680 445

For further information on recordkeeping contact:

- Information Management Services
  ICT Sustainability, Information and Technologies Branch
  Email: InformationManagement@det.qld.gov.au
  Website: Recordkeeping (DET employees only)

For further information on disclosure and amendment of personal information contact:

- Information Release Unit
  Legal and Administrative Law Branch
  Email: rti@det.qld.gov.au

For assistance on the department's Information Asset Register contact:

- Information Governance
  ICT Sustainability, Information and Technologies Branch
  Email: Policy.INFOMNGT@det.qld.gov.au
  Website: Information Asset Register (DET employees only)

For policy advice on this procedure, contact:

- Information Governance
  ICT Sustainability
  Email: Policy.INFOMNGT@det.qld.gov.au

Uncontrolled Copy Disclaimer