Information and Records Management - Procedures

Definitions

Please refer to the University's Glossary of Terms for policies and procedures.

1. Purpose of procedures

These procedures provide guidance and direction on the management of information and records throughout the information lifecycle.

2. Scope and application

These procedures apply to all University information and records, in all formats. These procedures are further supported by guidelines and other local documents as identified.

3. Information governance

Information management activities are delivered via annual Information Management Action Plans, overseen by the Information Management Committee. Minutes from these committee meetings are available on the Staff Intranet.

4. Information and records management

4.1 Corporate information and records must be captured by all staff and should provide reliable and accurate evidence of business decisions and actions. The University retains and disposes corporate information and records in accordance with the Public Records Act 2002 (Qld) and the relevant retention and disposal authorities.

4.2 All University records must be captured in an approved records management system. These approved systems appropriately support information and records management processes, and are secure from unauthorised access, damage and misuse. Corporate records must not be maintained in email folders, shared drives, personal drives or external storage media as these lack the necessary functionality. Endorsed systems for the storage of records are listed in Schedule A.

4.3 Endorsed systems for the storage of corporate information are listed in the ICT Security - Operational Policy, Schedule A – Business Systems. Guidelines on managing information in specific systems are available on the Staff Intranet.

4.4 To ensure University staff have access to the right information at the right time, regardless of location, all records stored in an endorsed system for the storage of records (see Schedule A) are required to be captured digitally.

- It is not necessary to attach paper copies of born-digital records to official folders.
- Add digitised copies of born-physical records and attach the physical record to the official folder. Born-physical records include documents containing wet signatures.

4.5 Staff should not dispose of records by either destruction, deletion, transfer, sale or donation, without prior approval from Information Management Services.

The timely disposal of information and records is essential for effective management. Some information can be destroyed in the normal course of business, staff should refer to the Managing Information pages on MyUniSC (staff login required).

Some records may be eligible for early disposal in accordance with the Disposal of Digitised Records – Procedures. Business areas seeking to undertake this activity should refer to this procedure and be guided by Information Management Services before starting any digitisation of original print records.

Corporate records are destroyed after fulfilling the minimum retention period set out in records authorities issued by the Queensland State Archives. Retention periods in records authorities take into account all business, legal and government requirements for the

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Head, Information Governance

FIRST APPROVED

22 September 2015

LAST AMENDED

9 November 2022

REVIEW DATE

22 September 2020

STATUS

Active

records. The University uses a number of general and agency-specific authorities to determine retention, destruction and transfer actions for its records.

Records determined to be of historical or cultural significance to the University can be retained for longer than the minimum period required. This includes records substantially contributing to the knowledge and understanding of aspects of University history, society, culture, environment and people. Assistance in determining records of this nature is available via Information Management Services, following criteria outlined by Queensland State Archives for substantial contribution to community memory.

5. Information accessibility

5.1 The University approach to information access is one of openness, encouraging a culture of information sharing to ensure organisational effectiveness. Where required by legislative and business requirements, access restrictions are applied to protect: individual staff or client privacy; sensitive material; and records requiring restricted access (in accordance with the University's information security environment).

5.2 Ownership of information, and records created or received during the course of business is vested in the University, unless otherwise agreed.

5.3 The University complies with the requirements of the Right to Information Act 2009 (Qld). It is committed to providing, as far as practical, an open environment which enables members of the public and the University community to access non-personal University information in the University's possession or under the University's control (unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended) without recourse to formal RTI applications. Information may also be released administratively on request.

Decisions as to the release of requested information that is not available on the University's website or in other publications are made within the guidelines of the RTI Act, taking into consideration the factors relating to exemptions and public interest. Organisations such as staff and student unions, sports associations and companies such as the Innovation Centre Pty Ltd are regarded by the University as independent for the purposes of RTI applications.

Applications for information not already available by other means must be made via the application form available. Processing of applications is conducted within the timeframes set out in the RTI Act. Fees and charges for formal applications, processing and access provision are applied as specified in the RTI Act. The RTI and Privacy Officer must provide to the applicant written reasons for decisions not to release documents or to give only partial access to documents. The Review Officer will internally review such decisions upon appeal by an applicant. Further review by the Queensland Right to Information Commissioner is also available.

6. Information Privacy

6.1 The University collects and uses personal information about its students, staff and others in order to operate effectively. Personal information held by the University is collected and managed in a responsible, secure manner, in compliance with the Information Privacy Principles outlined in the *Information Privacy Act*.

Access to personal information within the University is restricted to authorised staff with business process requirement. See Personal information – Guidelines (staff login required).

Under the *Information Privacy Act*, a person has the right of access to documents of the University that contain that person's personal information. A person also has the right to amend, if inaccurate, incomplete, out of date or misleading documents relating to their personal information. The University will release requested documents to an applicant unless on balance it is considered contrary to the public interest to do so, the documents are considered exempt under the Act, or documents are unable to be located.

Applications for access to, or amendments of, documents must be made via the application form available. Processing of applications is conducted within the timeframes set out in the Information Privacy Act. No charges apply for applications to access or amend a person's own personal information. Charges may apply for providing copies of requested information. The RTI and Privacy Officer must provide to the applicant reasons for decisions not to release documents or to give only partial access to documents. The Review Officer will internally review such decisions upon appeal by an applicant. Further review by the Queensland Privacy Commissioner is also available.

7. Information security

7.1 The University demonstrates a commitment to maintaining a robust information security environment, further addressed in the Information and Communication Technology (ICT) Security – Managerial Policy. For handling requirements related to information asset security, see Information asset security and handling – Guidelines.

PUBLIC AUDIENCE	INTERNAL AUDIENCE	INTERNAL AUDIENCE	INTERNAL AUDIENCE
Information intended for public use/consumption and intended for distribution outside the University.	Information intended only for all employees and approved non-employees of the University.	Information intended strictly for distribution/use by a select group.	Information that is extremely sensitive and intended for use only by various named individuals.
Public	Internal	Confidential	Restricted

The default information asset security classification is INTERNAL. Information assets that have not been specifically classified shall be deemed INTERNAL.

8. Information integrity

8.1 All information and records management practices in the University are to be in accordance with these procedures and related policy. Business processes must ensure the maintenance of reliable information and records. The operational management of information through the information lifecycle is promoted.

CREATE > STORE > USE & SHARE > ARCHIVE > DISPOSE
Maintain

8.2 Organisational information is created, collected, classified, and organised in a manner that ensures its integrity, quality and security. The Information Asset Register records organisational information asset metadata to assist with information asset management, classification, and planning. The register outlines information asset: security, content type, location/source system, Information Asset Steward, Information Asset Administrator, and other related metadata. To access the Information Asset Register, contact Information Management Services unit.

8.3 Whilst information re-use is encouraged, information duplication is discouraged. Staff should collaborate to prevent the storage of duplicate files, wherever possible referring to an organisational single source of truth rather than saving a local copy. The use of organisational templates is encouraged (accessed via the Staff Intranet).

8.4 Information and records management training is provided for University staff to the level of their responsibility under this policy, via the Information Management Services unit. Information management resources for staff are available on the Staff Intranet.

8.5 The University has a commitment to monitoring information practice compliance, and risk, via the Information Management Services unit.

8.6 A Records Disaster Recovery Plan is maintained to minimise the loss of University records in the event of a disaster.

9. Roles and responsibilities

Assigning responsibilities for information asset management ensures the information asset is appropriately identified and managed throughout its lifecycle and is accessible to appropriate stakeholders. These information roles and responsibilities are based on the wider Queensland Government Information management roles and responsibilities guideline (IS44), and as per requirements of the Right to Information Act 2009 (Qld) and Information Privacy Act 2009 (Qld).

9.1 General information and records roles and responsibilities

ROLE	RESPONSIBILITIES	APPOINTED BY
Information Asset Steward	Information asset management, authority and accountability. This includes ensuring: • Information asset value to the organisation is fully realised. • Information asset is shared to the maximum extent possible in accordance with security requirements. • Information asset quality is in line with business needs.	Information Management Committee

	• Business process for the information asset is established.	
Information Asset Administrator	Administration of information asset, as directed by the relevant Information Asset Steward. This includes: • Understanding the business process, value, security level, and risks of the information asset. • Monitoring information asset quality.	Information Asset Steward
Information Asset User	The correct management of information and records as defined by these procedures and related policy.	
Information Management Committee	Providing leadership, direction and strategic advice on the planning and delivery of the Information Management Strategy, Roadmap and Action Plan in alignment with the Planning Framework.	ICT Governance Committee
Cost centre managers	Visible support of and adherence to these procedures and related policy. This includes: • Ensuring staff are aware of, and are supported to follow, the information management practices defined in these procedures. • Ensuring all appropriate records within their area are recorded in an approved records management system. • Establishing business processes to locate information held in their areas for RTI and information privacy requests and updating areas under the Publication Scheme.	

9.2 Information privacy and RTI roles and responsibilities

ROLE	INFORMATION PRIVACY RESPONSIBILITIES	RTI RESPONSIBILITIES
Principal officer / Vice-Chancellor and President	Determining the outcome of applications made under the Information Privacy Act 2009 (Qld). The Vice-Chancellor and President has delegated this responsibility as per the Information Management Framework – Governing Policy.	Determining the outcome of applications made under the Right to Information Act 2009 (Qld). The Vice-Chancellor and President has delegated this responsibility as per the Information Management Framework – Governing Policy.
RTI and Privacy Officer / Head, Information Governance	Making initial decisions regarding release of documents within the time periods stipulated in the Information Privacy Act. In this function, the RTI and Privacy Officer may deal with prospective applicants and liaise with organisational units regarding access to documents.	Making initial decisions regarding release of documents within the time periods stipulated in the RTI Act. In this function, the RTI and Privacy Officer may deal with prospective applicants and liaise with organisational units regarding access to documents.
RTI and Privacy Coordinator / Administration & Finance Officer, Library Services	Assisting the RTI and Privacy Officer in the related duties.	
Cost centre managers	Establishing business processes to locate information held in their areas. In the event that information cannot be located, a written explanation of what steps have been taken to locate them must be provided to the RTI and Privacy Officer.	Establishing business processes to locate information held in their areas. In the event that information cannot be located, a written explanation of what steps have been taken to locate the information must be provided to the RTI and Privacy Officer. Updating information relating to their units under the Publication Scheme.
Review Officer / Deputy Vice-Chancellor (Academic)	Formal internal reviews of decisions made by the RTI and Privacy Officer, if requested by the applicant.	

END

Schedule A: Endorsed systems for the storage of records

RECORD TYPES	SYSTEM
Staff records, student records.	Objective ECM or PeopleSoft or Techone ECM
Legal records, contractual records, and administrative records.	Objective ECM or Techone ECM
Records associated with the Policy Repository	Recfind
Work integrated learning (WIL) records and Off-campus Activities records	Sonia
Financial records	TechOne

RELATED DOCUMENTS

- Disposal of Digitised Records - Procedures
- Information Management Framework - Governing Policy

LINKED DOCUMENTS

- Information Management Framework - Governing Policy

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2002 (Qld)
- Queensland Information Standards
- Information Privacy Act 2009 (Qld)