Information and Records Management - Procedures

1. Purpose of procedures

1.1 These procedures operationalise the Information Management – Governing Policy and support the effective management of information assets and records throughout the information lifecycle.

1.2 This policy document must be read in conjunction with the linked Information Management – Governing Policy.

2. Scope and application

2.1 These procedures apply to all staff and other individuals working for, or on behalf of, the University and relates to all University information assets and records, in all formats and locations.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

4. Information lifecycle management

4.1 Information assets, whether physical or digital, have intrinsic value and are fundamental to the day-to-day activities of the University.

4.2 Information assets must be appropriately managed throughout the information lifecycle phases:

(a) creation, collection, capture;

(b) store, classify, secure;

(c) retention, archiving; and

(d) disposal, destruction.

4.3 Records are a form of information asset, retained as evidence of business activities, transactions, or decisions. Records are specifically addressed in the *retention, archiving* and *disposal, destruction* phases of the information lifecycle.

4.4 Creation, collection, capture

4.4.1 Information assets are created by staff or other individuals working for, or on behalf of, the University or are collected from individuals or third-parties.

4.4.2 Information assets must be created or collected accurately, reliably, and completely to support University operations, enhance business efficiencies and decision-making, uplift accountability, promote transparency, mitigate risks, and improve organisational memory.

4.4.3 Information assets provide reliable and accurate evidence of business decisions and actions. Both physical and digital information assets must be captured and managed in University-controlled environments.

4.5 Store, classify, secure

4.5.1 Information assets must be securely stored in fit-for-purpose University-managed environments, systems, and locations in accordance with the ICT Security - Operational Policy.

4.5.2 Information assets must be discoverable so they can be accessed, understood, and used. Discoverability is achieved through capturing metadata about information assets. The University's Information Asset Register documents organisational information asset metadata to assist with information asset management and classification.

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Chief Data Officer

FIRST APPROVED

22 September 2015

LAST AMENDED

2 January 2024

REVIEW DATE

8 December 2025

STATUS

Active

4.5.3 Digitisation of physical information assets including records assists with discoverability. Business areas seeking to undertake digitisation activities should refer to the Disposal of Digitised Records – Procedures and be guided by the Insights and Analytics Unit before starting any digitisation of physical information assets.

4.5.4 Information assets must be stored and protected according to risk profile, value, and use.

4.6 Retention, archiving

4.6.1 The University retains records for as long as required, in accordance with the *Public Records Act 2002* (Qld) and the relevant retention and disposal schedules administered by Queensland State Archives.

4.6.2 Records determined to be of archival or enduring value to the University can be retained for longer than the minimum period required. This includes records that substantially contribute to the knowledge and understanding of aspects of University history, society, culture, environment, and people. Assistance in determining archival or enduring value is available via the Insights and Analytics Unit, following Queensland State Archives criteria.

4.7 Disposal, destruction

4.7.1 The Insights and Analytics Unit centrally manages the disposal of records for the University. The disposal of records by destruction, deletion, transfer, sale or donation must first be approved by the Insights and Analytics Unit.

4.7.2 University records are disposed following a prescribed process, once the minimum retention period set out in schedules administered by Queensland State Archives is met. The University uses general and agency-specific schedules to determine its retention, disposal, and transfer actions and observes all business, legal and government requirements.

4.7.3 The decommissioning of University business systems, and the appropriate handling or migration of information assets and metadata contained in those systems, must be completed with support from the Insights and Analytics Unit following the Business System Decommissioning Pathway process.

4.7.4 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 these procedures and be guided by the Insights and Analytics Unit before starting any digitisation of original print records.

4.7.5 Once approved for disposal, records must be securely destroyed via the method most appropriate for the record format and security classification. The appropriate destruction of records must be documented and captured in an approved records management system.

5. Records management

5.1 Records management is a legislative obligation of the University and must be done so in accordance with the *Public Records Act 2002* (Qld) and directions issued by the State Archivist and Queensland State Archives.

5.2 A record can be in any format, including (but not limited to) hard-copy or physical and electronic or digital documents, emails, instant messages, maps, phone messages, oral conversations, videos, photos, and building plans.

5.3 Records provide evidence of the University's actions, activities, and decisions. Records reflect what happened, when it happened, who was involved, resolutions or recommendations, advice, or instruction.

5.4 Vital records are information assets that are required for the University to continue operations. The University identifies and documents its vital records in the University's Information Asset Register.

5.5 University records must be captured and managed 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.

Table 1: Current endorsed Records Management Systems.

RECORD TYPES	SYSTEM
Staff records, student records.	PeopleSoft or TechOne ECM
Legal records, contractual records, and administrative records.	TechOne ECM
Records relating to policy and policy approval	RecFind
Work integrated learning records.	Sonia
Financial records	TechOne

6. Information access, use and sharing

6.1 The University approach to information access is one of openness, encouraging a staff culture of information sharing to ensure organisational effectiveness.

6.2 Where required by legislative and business requirements, access restrictions are applied to protect individual staff or client privacy, sensitive material and information assets requiring restricted access (in accordance with the University's information security environment).

6.3 Ownership of information and records created or received during the course of business is vested in the University, unless otherwise agreed. See the Intellectual Property - Governing Policy.

6.4 To ensure staff have timely access to the right information, the University has a preference for 'born digital' information assets and records. Wherever practical, information assets and records should be created or captured and maintained in a digital format.

6.5 Where business processes result in physical information assets being created, including documents containing wet signatures, records may be digitised in accordance with the Disposal of Digitised Records – Procedure, under the guidance of the Insights and Analytics Unit.

6.7 Right to Information (RTI)

6.7.1 The University complies with the requirements of the *Right to Information Act 2009* (Qld) (RTI Act).

6.7.2 Decisions as to the release of requested information that is not available on the University's website or in other publications are made by the Right to Information and Privacy Officer (RTI and Privacy Officer) and in line with the requirements of the RTI Act, taking into consideration the factors relating to exemptions and public interest. Organisations such as staff and student unions and sports associations are regarded by the University as independent for the purposes of RTI applications.

6.7.3 Applications for information not already available by other means the must be made via the application form available from the Queensland Government. See Right to Information webpage.

6.7.4 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.

6.7.5 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.

7. Information privacy

7.1 The University collects and uses personal information about its students, staff and others in order to operate effectively. See Privacy webpage.

7.2 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 2009* (Qld).

7.3 In some circumstances, the University may share information with third-party providers, or a third-party may collect personal information for, or transfer personal information to, the University. When a third-party will in any way deal with personal information for the University, the University will take reasonable steps to ensure third-party agreements require the third party to comply with the Information Privacy Principles contained in the *Information Privacy Act 2009* (Qld) or *Privacy Act 1988* (Cth), and where possible, require the third-party to de-identify personal information.

7.4 The University may transfer personal information to third parties, particularly third-party service providers, outside Australia, including (but not limited to) the United States of America and countries in the European Union. The University takes appropriate steps to ensure that recipients of personal information are required to maintain confidentiality, that measures are implemented to ensure any transferred personal information remains secure, and is compliant with the *Information Privacy Act 2009* (Qld) and relevant Data Protection Laws.

7.5 Access to personal information within the University is restricted to authorised staff with business process requirements. See Personal information – Guidelines.

7.6 Under the *Information Privacy Act 2009* (Qld), 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.

7.7 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 *Information Privacy Act 2009* (Qld), or documents are unable to be located.

7.8 Applications for access to, or amendments of, documents must be made via the application form available from the Queensland Government.

7.9 Processing of applications is conducted within the timeframes set out in the *Information Privacy Act 2009* (Qld). No fees apply for applications to access or amend a person's own personal information. Charges may apply for providing copies of requested information.

7.10 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.

7.11 The Review Officer will internally review such decisions upon appeal by an applicant. Further review by the Queensland Privacy Commissioner is also available.

8. Security

8.1 The University demonstrates a commitment to maintaining a robust information security environment, further addressed in the ICT Security – Operational Policy. For handling requirements related to information asset security, see Information Asset Security and Handling – Guidelines.

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

Table 2: Information asset security classifications

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

8.3 Data breach

8.3.1 A data breach occurs when personal information is accessed or disclosed without authorisation, or is lost. A data breach can involve digital or physical information assets, as well as verbal disclosure. A data breach may be due to a cyber security incident, accidental disclosure, malicious activity, or third party breach of UniSC information assets.

8.3.2 The University has a data breach response plan that sets out the actions to be taken in the event of a data breach in alignment with the Critical Incident Management - Governing Policy. The Data Portal provides further information on reporting a data breach (staff login required).

9. Information integrity

9.1 Information assets are created, collected, classified, and organised in a manner that ensures their integrity, quality and security.

9.2 Responsible reuse of information is encouraged, and duplication of information assets is to be avoided. Staff should collaborate to prevent the storage of duplicate files, wherever possible using an organisational single source of truth rather than saving a local copy. The use of organisational templates is required accessed via the Staff Intranet (staff login required).

9.3 Information and records management training is provided for staff, via the Insights and Analytics Unit. Information and records management resources for staff are available on the Staff Intranet (staff login required).

9.4 The University has a commitment to monitoring information and records management compliance and risk, via the Insights and Analytics Unit.

9.5 Disaster Recovery Plans for both physical and digital information assets are maintained to minimise the loss of University records in the event of a disaster.

10. Roles and responsibilities

10.1 Assigning responsibilities for information asset management ensures the information asset is appropriately identified and managed throughout its lifecycle and is accessible to appropriate stakeholders.

Table 3: General information and records roles and responsibilities.

ROLE	RESPONSIBILITIES	ROLE HOLDER
Data Champion	Enterprise-level authority and accountability under legislation for the collection and management of the University's data and information.	Vice-Chancellor and President
Information Asset Custodians	Defines strategic uses of information and is responsible for ensuring information assets are managed in compliance with legislative and regulatory obligations, and University policy documents.	Senior Staff
Information Stewards	Ensures quality and integrity of information by ensuring information management is embedded in the daily operation of processes and systems. Processes and systems can be digital or physical.	Managers, System Administrators
Information User	Chooses the best source of information to meet their needs.	All individuals who access information

Table 4: Information privacy and RTI roles and responsibilities

ROLE	INFORMATION PRIVACY RESPONSIBILITIES	RTI RESPONSIBILITIES
Principal officer or Vice-Chancellor and President (VCP)	Determining the outcome of applications made under the *Information Privacy Act 2009* (Qld). The VCP has delegated this responsibility as per the Information Management – Governing Policy.	Determining the outcome of applications made under the *Right to Information Act 2009* (Qld). The VCP has delegated this responsibility as per the Information Management – Governing Policy.
RTI and Privacy Officer or Senior Lead – Privacy, Records & Data 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.
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 or Deputy Vice-Chancellor (Academic)	Formal internal reviews of decisions made by the RTI and Privacy Officer, if requested by the applicant.	

END

RELATED DOCUMENTS

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

LINKED DOCUMENTS

- Information Management - Governing Policy

RELATED LEGISLATION / STANDARDS

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