Records Management - Procedures

1. Purpose

1.1 These procedures operationalise the University's principles of data governance and ensures that full and accurate records of all University activities, transactions and decisions are created, managed, retained, and disposed of in accordance with the legislative requirements of the *Public Records Act 2023 (Qld)*.

1.2 These procedures must be read in conjunction with the linked Data Governance – Operational Policy, Data Management - Procedures, Data Classification - Procedures, Digitisation of Physical Records – Guidelines (login required) and Disposal of Records – Guidelines (login required).

2. Scope and application

2.1 These procedures apply to all University staff, students undertaking research or involved in other University business, approved third parties, alumni, contractors, and sub-contractors. It includes all individuals who handle University data and information, regardless of their role or affiliation.

2.2 These procedures apply to all University data and information.

3. Definitions

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

3.2 The terms data and information are used interchangeably within this policy, recognising the overlap between the two. In their simplest form, data is often considered as raw values and individual facts in any form, and information is data that has been contextualised. Both data and information can be University records.

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Chief Data Officer

FIRST APPROVED

22 September 2015

LAST AMENDED

3 December 2024

REVIEW DATE

3 December 2026

STATUS

Active

4. Identification of records

4.1 Records are any form of data or information, including documents in digital or physical form, that capture evidence of a University decision, transaction or activity and therefore have a retention requirement under the *Public Records Act 2023 (Qld)*.

4.2 Records can be categorised as high-value or high-risk. Information that the University would have considerable difficulty operating without are considered high-value records and those that would result in significant risk to the University should they be lost, damaged, or deleted prematurely, are deemed high-risk records.

4.3 Examples of records include:

(a) any data or information vital to business continuity;

(b) data and information pertaining to historical, cultural or legal matters;

(c) student and employee details;

(d) course and study information;

(e) contracts, agreements, Memorandum of Understanding (MOU) and other legal documents;

(f) financial information;

(g) strategic and operational plans;

(h) project management documentation.

5. Managing records through the data lifecycle

5.1 Records management aligns with the stages of the University's data lifecycle depicted in Figure 1: Data lifecycle, and in accordance with Data Governance – Operational Policy and Data Management - Procedures.

Figure 1: Data lifecycle

5.2 Capture

5.2.1 Complete and reliable records must be captured in a University approved business system (login required), including relevant metadata to ensure discoverability and integrity. Metadata can include:

(a) dates;

(b) business area;

(c) people, processes;

(d) events;

(e) relationships to other records; and

(f) legal context.

5.2.2 All high-value and high-risk records, along with any other record that has a minimum retention period must be captured within the approved University records management system, Technology One Enterprise Content Management (T1ECM).

5.2.3 Records created in digital format must remain digital, adhering to the concept of ‘born digital, stay digital’ in the management of records. Physical copies of ‘born digital’ records must not be kept.

5.2.4 Ownership of records created or received during the course of business is vested in the University unless otherwise agreed.

5.3 Store

5.3.1 Digital records must be stored within T1ECM when they are no longer in day-to-day business use. This ensures that minimum retention periods and disposal are managed and controlled in accordance with legislative requirements. The storage of contracts in T1ECM is exempt, as they must be captured in the Contracts Register (login required).

5.3.2 Physical records must be stored in either an on-site University approved secure location or an approved off-site storage facility, which is coordinated through the Records Management team. This includes any records that are managed as part of outsourced contractual arrangements. A record of their storage and associated context must be included in T1ECM.

5.3.3 Where practicable, physical records should be digitised to improve discoverability and accessibility in accordance with the Digitisation of Physical Records – Guidelines (login required). Some physical records can be disposed of once they have been captured as a digitised copy in T1ECM. Disposal must be facilitated by the Records Management team (login required).

5.4 Utilise

5.4.1 Storing records in T1ECM increases the value of the information as a strategic asset through discoverability and access.

5.4.2 When utilising records, it is imperative that the integrity and quality of information is maintained. This includes ensuring that the information is current, correct and up to date. Records should be used in such a way as to maintain the intent of the information provided and ensure all changes or modifications are audited and discoverable.

5.4.3 Duplication of the record should be avoided. Use links to the record rather than creating and sending a copy. Versioning and version control should be maintained to manage changes or modifications.

5.4.4 When possible, physical records should be digitised and used in digital format. The use of physical records as part of a business process should be avoided.

5.5 Share

5.5.1 Records must have the appropriate level of access control applied, to enable secure sharing of information that protects privacy and confidentiality, in accordance with the Data Classification - Procedures, legislative requirements and business needs.

5.5.2 These controls are balanced with the University’s approach for openness to enhance discoverability of records, encouraging a culture of information sharing to ensure organisational effectiveness.

5.6 Archive

5.6.1 Capturing records within T1ECM ensures that records are retained for the correct length of time, according to the retention and disposal schedules administered by Queensland State Archives, in accordance with the *Public Records Act 2023 (Qld)*.

5.6.2 Records can be retained for longer than the minimum period required, when they are determined to be of archival or enduring value to the University. This includes records that substantially contribute to the knowledge and understanding of aspects of university

history, society, culture, environment, and people. Guidance should be sought from the Records Management Team on records of archival or enduring value.

5.7 Dispose

5.7.1 The disposal of records encompasses the:

(a) destruction of physical records;

(b) erasure of digital records; or

(c) transfer of digital or physical records.

5.7.2 The Records Management Team must have confirmed the following requirements prior to the disposal of records (digital or physical):

(a) records have met the minimum retention period under the retention and disposal schedule administered by Queensland State Archives, in accordance with the *Public Records Act 2023 (Qld*);

(b) records are confirmed as having no further business need, including under Right to Information requests or as evidence in current or pending legal proceedings;

(c) records are approval for disposal by the Executive Officer under the *Public Records Act 2023 (Qld)*, as identified in Delegations Schedule B.

5.7.3 Records disposal must in in accordance with the Disposal of Records – Guidelines (login required), and overseen by the Records Management Team (login required). This includes ensuring that evidence that demonstrates all requirements for disposal were met is captured in T1ECM.

5.7.4 Ensuring all records with minimum retention requirements as stipulated by legislative requirements, including high-risk and high-value records are held in T1ECM, guarantees that records are retained for the correct length of time, reducing the risk of accidental or premature disposal.

5.7.5 Physical records that have been digitised can be eligible for disposal if retention of the physical form is not required for artistic or artefactual value or to meet a legislative requirement. Guidance must be sought from the Records Management Team (login required) prior to physical records disposal.

5.7.6 When University approved business systems are decommissioned the Records Management Team (login required) must approve and oversee the appropriate disposal of the data and information.

6. Monitoring and Reporting

6.1 Regular monitoring and reporting on the application of record keeping practices as defined in these procedures is reported to the Data Analytics and Information Management Advisory Committee.

6.2 The Chief Data Officer reports on University compliance with these procedures in accordance with the Compliance Management Framework - Governing Policy.

6.3 The Records Management Team monitors the opertations within the T1ECM system to ensure compliance with records entry, application of retention periods and the integrity and security or records and reports to the Chief Data Officer on compliance.

7. Authorities and responsibilities

7.1 As the Approval Authority the Chief Operating Officer approves these procedures to operationalise the Data Governance – Operational Policy.

7.2 As the Responsible Executive Member the Chief Operating Officer can approve guidelines to further support the operationalisation of these procedures. All procedures and guidelines must be compatible with the provisions of the policy they operationalise.

7.3 As the Designated Officer the Chief Data Officer is authorised to approve associated documents to support the application of these procedures.

7.4 These procedures operate from the last amended date, and all previous iterations of policy documents on records management are replaced and have no further operation from this date.

7.5 All records relating to records management must be stored and managed in accordance with the Data Governance – Operational Policy.

7.6 These procedures must be maintained in accordance with the Policy Framework – Procedures and reviewed on a shortened 2-year policy review cycle.

7.7 Any exception to this policy to enable a more appropriate result must be approved in accordance with the Policy Framework – Procedures prior to any deviation from these procedures.

7.8 Refer to Schedule B and Schedule C of the Delegations Manualin relation to the approved delegations detailed within these procedures.

7.9 Records Management Roles

7.9.1 The following roles, responsibilities and accountabilities are specific to these procedures and cascade from the high-level roles and responsibilities in the Data Governance – Operational Policy.

ROLE	PERSON	RESPONSIBILITY AND ACCOUNTABILITIES
Data Champion	Vice-Chancellor and President	Executive Officer under the *Public Records Act 2023 (Qld)* and accountable for compliance with legislation, including approving disposal of records.
Chief Data Officer	Chief Data Officer	Authorised delegate for the Vice-Chancellor and President including approving disposal of records. Accountable for: (a) risk assurance for records related risks. Responsible for: (a) embedding procedural and legislative requirements for records management; (b) appointing and inducting Data Custodians; (c) oversight of the records management system, T1ECM; and (d) implementing procedures and supporting guidance to embed responsible and compliant records management practices.
Data Custodians	Heads of Departments (appointed by the CDO)	Accountable for: (within their data domain) (a) ensuring records are correctly managed within their data domain. Responsible for: (a) overseeing and implementing record keeping processes in their business area; (b) nomination of subject matter experts and ongoing support for their role; and (c) embedding appropriate use of University approved business systems and T1ECM.
Business System Owners	In accordance with the ICT Security - Operational Policy	Responsible for: (a) implementing and reviewing technical controls, including for security and access, to protect and maintain university records within approved business systems throughout their lifecycle.
Data Subject Matter Experts	Staff based on specific expertise-criteria relative to a data asset	Responsible for: (a) providing expertise for business considerations relating to University records.
Data Users	All University staff, affiliates or groups that create or use data.	Responsible for:

(a) capturing accurate and complete records and associated metadata relating to their day-to-day work in the appropriate University approved business system; and

(b) adhering to these procedures.

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Procedures

- Compliance Management Framework - Governing Policy
- Copyright - Academic Policy
- Data Breach - Procedures
- ICT Access Control - Operational Policy
- ICT Security - Operational Policy
- Information System Operations - Procedures
- Intellectual Property - Academic Policy
- Privacy and Right to Information - Operational Policy
- Privacy Management - Procedures
- Right to Information - Procedures
- University Policy Documents - Procedures

LINKED DOCUMENTS

- Data Classification - Procedures

- Data Governance - Operational Policy
- Data Management - Procedures

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Queensland Information Standards
- Information Privacy Act 2009 (Qld)