Information Management Procedure

Version 2 – Reconfirmed 5 July 2024

Contents

Purpose

This procedure describes the recordkeeping and information management requirements for University business and operational records in accordance with the *Archives Act 1983 (Tas)*.

Applicable governance instruments

Instrument	Section	Principles
Data and Information Governance Policy	1 Privacy 4 Data and information management	1.1 – 1.7 4.1 – 4.4
Compliance Policy	4 Access to information and disclosures	4.1 – 4.2
Archives Act 1983 (Tas)		
Right to Information Act 2009 (Tas)		
Privacy Act 1988 (Cth)		
Personal Information Protection Act 2004 (Tas)		

Procedure

1. Introduction

1.1. The objectives of the University's recordkeeping and information management requirements are to ensure that:

a. information assets are formally, proactively and efficiently managed to meet strategic objectives

b. the associated risks are consistently and effectively managed

c. the University complies with the requirements of the *Archives Act 1983 (Tas)*.

1.2. The Vice-Chancellor and the University Executive Team have overall responsibility for ensuring the University fulfils its legal and business obligations regarding business records and information management.

1.3. This procedure does not apply to research data or research outputs, but does apply to business and operational records related to research data and research outputs. For the management of research data, see the *Research Data Management Procedure*. For management of and access to research outputs, see the *Open Access Procedure* and *Publication and Dissemination of Research Procedure*.

2. Records and information management

2.1. Ownership of all University business and operational records and information is vested in the University. Any change to custody must be undertaken in consultation with Office of the State Archivist (OSA).

2.2. All University business and operational records and information, excepting short term or records of transitory value, (for examples see the Staff Recordkeeping Manual - Ephemeral Records), will be captured in a compliant Electronic Document and Records Management System or compliant University supported business information system. The system used will support the information lifecycle and minimum retention periods provided in the authorised retention and disposal schedules.

2.3. All business information systems will be assessed to ensure that the system meets the requirements of a compliant recordkeeping system. Recordkeeping systems within the University will:

a. preserve complete and fixed impressions of records;

b. register records and their associated metadata;

c. protect records and metadata from deletion and/or tampering;

d. secure and restrict access to records;

e. provide an audit trail and revision history for records and their metadata; and

f. ensure records remain accessible over time.

Instructions can be found at: Checklist for assessing business information systems and the Staff Recordkeeping Manual – Recordkeeping Systems.

2.4. All University contracts and agreements, where the University is a signatory participant, will be created, captured, securely stored, accessed, retained and disposed of in accordance with Staff Recordkeeping Manual – University Contract Recordkeeping instructions.

3. Education and training

3.1. All employees, contractors, consultants and volunteers will make and keep full and accurate records of business activities they undertake in the course of their employment. Obligations are outlined in the Staff Recordkeeping Manual – Recordkeeping Responsibilities.

3.2. New employees will undertake the Recordkeeping at the University of Tasmania online tutorials as part of their induction.

3.3. Heads of organisational units will ensure employees are equipped to establish and resource appropriate recordkeeping and are responsible for disposal of records in accordance with authorised disposal schedules, and certification of entries made in each of the business units' Register of Records Destroyed.

3.4. Support, education and training material can be found at: Information Management and Service Portal Tips and Tricks.

Requests for assistance relating to records and information can be made at:

- Service Portal > Information Management
- IMU.Staff@utas.edu.au

4. Access to business and operational records and information

4.1. University business and operational records and information will be accessible for as long as required to meet accountability, legal, administrative, financial, research and community requirements and expectations.

4.2. Where required by regulatory compliance instruments and business requirements, including senior management directives, access restrictions will be applied to selected records and information to protect an individual's privacy or to protect the University's interests.

4.3. Security classifications will be applied to records and information to identify appropriate accessibility and storage requirements (see section 5).

4.4. Business and operational records and information held by the University may be accessed by informal or formal request.

4.5. Where information is sought by way of assessed disclosure under the *Right to Information Act 2009* (Tas) the University may exercise its right not to disclose the requested information, subject to the limitations of the legislation. In this case an authorised delegate (Right to Information Officer) must make this assessment.

4.6. Further details concerning access or Right to Information is available from the University's website.

5. Classification and metadata

5.1. All University business and operational records and information are to be security classified according to the UTAS Data Classification Framework and managed according to the minimum requirements for the classification level.

5.2. All University business and operational records and information should be classified according to the University's Business Classification Scheme (BCS). The BCS is based on the operational activities of the University and is directly linked to the authorised Retention and Disposal Schedules. The BCS is integrated with the University Electronic Document and Records Management System, Content

Manager (TRIM), and can be extended effectively to an intranet, extranet, network drive folders, email folders, and/or other personal and workgroup systems.

5.3. Naming conventions and titling of records and information must be consistent and conform to industry or domain-specific metadata standards and the University's Data Entry Standards.

6. Storage

6.1. Physical and electronic information must be stored in repositories that are appropriate for the classification level of the data (see sections 5.1 and 5.2) and the business requirements. Where possible, research data should not be stored in repositories intended for business and operational information and vice versa. University storage repositories must be compliant with those standards and guides issued by the State Archivist and instructions listed in the Staff Recordkeeping Manual – Storage Areas.

6.2. Off-site commercial storage facilities used to store inactive records and information must be certified by the Office of the State Archivist. All inactive records must be listed in a Register of Inactive Records prior to transfer to assist retrieval.

6.3. A risk assessment must be undertaken when choosing to utilise Cloud or external solutions for the storage of electronic records and information, to ensure compliance with all legislative and business requirements, as outlined in the *Cyber Security Controls Procedure*.

7. Retention and disposal

7.1. In accordance with the *Archives Act 1983*, University records and information are not to be destroyed without authorisation from the State Archivist.

7.2. All organisational units will use relevant authorised Retention and Disposal Schedules for the purposes of appraisal, retention and disposal of University records and information, irrespective of format and storage location. These authorities are accessible from the Information Management – Retention and Disposal Schedules.

7.3. Changes to legislation, standards or business processes impacting on minimum retention requirements stipulated in current University Disposal Schedules must be communicated to the Information Management Unit (IMU) to ensure schedules remain appropriate for the University.

7.4. Organisational units are required to undertake an annual review of their records and information to identify and appraise University records and information eligible for disposal, (retention, migration, transfer or destruction).

7.5. Records and information of ephemeral / short term value may be destroyed in accordance with normal administrative practice outlined in the Staff Recordkeeping Manual – Ephemeral Records. Organisational Units will submit a Records Disposal Audit - Nil Return to IMU if there have not been any records and information destroyed during the year.

7.6. All University records and information of temporary value (with the exception of ephemeral / short-term value records) having met their minimum retention requirements will be listed in a Request for Destruction form and submitted to IMU **prior** to destruction.

7.7. All University records that have a permanent value and are identified as requiring transfer as a State Record must be transferred no later than 25 years after their closure/ceasing to be of

reference or authorisation was sought from the State Archivist to retain the records. For further information's see Staff Recordkeeping Manual – Transferring Records.

7.8. The approved Register of Records Destroyed will be retained for audit, legal and other business needs in accordance with the authorised Retention and Disposal Schedules.

7.9. Matters requiring interpretation of the relevant Retention and Disposal Schedules will be referred to IMU for investigation and advice.

7.10. Destruction of hardcopy and digital records and information will be undertaken in accordance with instructions outlined in the Staff Recordkeeping Manual – Destroying Records.

7.11. Source records and information that have been copied, converted or migrated from one format to another will be managed in accordance with requirements stipulated in DA 2159 – Disposal Schedule for Source Records.

7.12. Decommissioning or migration of business applications / systems will be undertaken in consultation with the Office of the State Archivist to ensure information contained in the system is retained in accordance with minimum retention requirements. Business system owners will liaise with IMU and complete the Decommissioning Business Information Systems Checklist **prior** to migration or decommissioning of the system.

7.13. The University is legally required to submit any publications (physical or electronic) it publishes if sold or otherwise distributed to the public for legal deposit with Libraries Tasmania and the National Library of Australia. Instructions can be found in the Staff Recordkeeping Manual – Legal Deposit of Publications.

8. Digitisation and disposal of physical source records

8.1. Physical source records meeting the requirements set out in the regulatory compliance instruments and the current Retention and Disposal Schedule authority, will be eligible for early destruction after scanning into a compliant recordkeeping system or a University supported business system.

8.2. A digitisation plan is required to demonstrate a considered approach to meeting conditions and requirements. Refer to the Staff Recordkeeping Manual – Scanning Records for instructions.

9. Records affected by disaster or malicious attack

9.1. The University will notify the State Archivist and complete an incident report whenever records and information have been damaged, lost or partially lost due to disaster such as flood, fire, cybersecurity, or malicious attack. Further information can be found in the Staff Recordkeeping Manual – Reporting Data Breaches / Incidents, the *Cyber Security Controls Procedure* and *Data Breach Procedure* including mandatory reporting of privacy and cybersecurity breaches and the required timeframes.

10. Non-compliance with the Archives Act

10.1. Non-compliance with the *Archives Act* must be reported through to the University's Compliance team and registered on the Non-Compliance Register. Non-compliances are then reported to the Audit and Risk Committee.

Related procedures

Research Data Management Procedure

Open Access Procedure

Cyber Security Controls Procedure

Data Breach Procedure

Versions

Version	Action	Approved by	Business Owner/s	Approval Date
Version 1	Approved	Chief Operating Officer	Chief Information Officer	10 June 2021
Version 1	Reconfirmed, unchanged	Chief Operating Officer	Chief Information Officer	30 June 2022
Version 2	Approved	Head of Student Services and Operations	Chief Information Officer	10 July 2023
Version 2	Reconfirmed, unchanged	Deputy Vice-Chancellor (Student Services and Operations	Chief Information Officer	5 July 2024

Definitions

Information Management Glossary