Records Management Policy

1. Purpose

1.1 The Records Management Policy (the policy) provides a framework to ensure full and accurate records are created, captured and managed for all UTS activities, in compliance with the State Records Act 1998 (NSW) (State Records Act).

2. Scope

2.1 This policy applies to all UTS staff and affiliates (hereafter staff).

3. Principles

3.1 UTS is committed to accountable business practices, including recordkeeping, and compliance with the State Records Act and other legislated recordkeeping requirements.

3.2 UTS recognises that the proper creation, capture, management, storage and protection of records in all formats:

- supports and enhances the university's activities
- facilitates decision-making
- protects the interests of the university
- protects community and public interests including privacy and information access obligations, and
- provides a record of the university's activities for future reference.

3.3 Recordkeeping requirements and practices will be embedded into UTS business activities, data governance, cybersecurity and information systems and processes.

3.4 Records management practices will be sustainable (refer Sustainability Policy), efficient and effective within the limits of legislative obligations, ensuring that accountability and compliance requirements are satisfied.

4. Policy statements

UTS records management program

4.1 All records created or received by UTS staff in the course of the university's operations and activities, including where an activity is outsourced or supported by a service provider, are owned by UTS.

4.2 UTS will establish and maintain a records management program (the program) that complies with the requirements of the State Records Act and its associated standards, policies and guidelines.

4.3 The program is mandatory and must be implemented by all business units, faculties, offices, institutes, centres or equivalent (hereafter unit) when the unit is first established. The program must be implemented in consultation with University Records.

4.4 Staff must be aware of and participate in the program through the creation, capture, management and protection of full and accurate university records.

4.5 To effectively maintain the program, units under their director (or dean or equivalent (hereafter director)) must:

- ensure that all staff are aware of the records management requirements outlined in this policy, the program and the approved recordkeeping systems used by the unit
- assign and maintain appropriate administrative support and records contact roles in line with this policy and the program
- regularly monitor recordkeeping practices through mandatory self-assessments to ensure ongoing compliance and sustainability
- develop and maintain a local records management plan that supports their local practices and incorporates any actions arising from self-assessment activities (except where these practices are already covered by a broader unit-level records management plan)
- embed recordkeeping requirements in relevant business processes and procedures.

4.6 Where a unit is being restructured, University Records must be consulted in advance to plan and facilitate the proper management, transfer, archiving or disposal of records as appropriate.

Recordkeeping systems

4.7 Records of the university must be captured as soon as practicable in a university recordkeeping system (see definitions).

4.8 The primary recordkeeping system at UTS is Content Manager (formerly known as TRIM). This recordkeeping system has been implemented as part of the program. Where other information systems are used to create and manage records, these must be assessed as a suitable recordkeeping system as required by this policy (see Recordkeeping in information systems (SharePoint, staff only)).

4.9 Information systems stewards (refer Data Governance Policy) are responsible for:

- ensuring information systems under their responsibility are assessed for recordkeeping compliance in line with this policy, and
- approving and communicating procedures or guidance that outline recordkeeping compliance requirements for the operation and management of that recordkeeping system (on the advice of the data steward).

4.10 Information systems must be reassessed for recordkeeping compliance if they undergo major upgrades or changes in functionality or content, including where a system may move from UTS to a service provider.

4.11 Obligations relating to access, security and data retention will still apply to information systems that are not being used as a recordkeeping system.

4.12 Records migrated to new information systems must be transferred in a manner that maintains the integrity, accuracy and context of the records and associated metadata. The migration must be clearly documented.

4.13 Final documents and records of completed activities or business processes must not be altered or removed from recordkeeping systems unless in line with the university's procedures (see Archiving and destroying records (SharePoint, staff only)) and/or required by law.

4.14 Digitising paper records is UTS's preferred way for units to capture and manage records of the university. Scanning activities must be undertaken in line with the university's procedures (see Scanning paper records (SharePoint, staff only)).

Vital records and contract management

4.15 Original vital records must be lodged with University Records within one month of the record and/or record variation being signed, approved or received, in line with the university's vital records program (SharePoint, staff only).

4.16 Data about contracts that is required to be reported by the university under the Government Information (Public Access) Act 2009 (NSW) (GIPA Act) must be provided to University Records within one month of contract execution, commencement and/or variation in line with procedures issued by University Records (see Right to information (Staff Connect)).

4.17 UTS will include details of these contracts on its public Register of contracts.

Record security and access

4.18 All records, and corporate data as defined under the Data Governance Policy, must be allocated one of the four following security classifications as outlined in the Information Security Classification Standard (available at Information security (SharePoint, staff only)):

- Public
- Internal
- Sensitive
- Confidential

4.19 Records that are classified as internal, sensitive or confidential must not be provided to external parties unless appropriately authorised. Further to provisions in this policy, details on access are also available in the Delegations, Privacy Policy, Privacy Management Plan (available at Privacy regulations) and Data Governance Policy.

4.20 All records must be stored in a secure location, with access provided in line with the security classification level applied.

4.21 Staff are responsible for ensuring records created or received via personal devices or programs are protected from unauthorised access or disclosure and are moved into the appropriate university recordkeeping system. Further requirements for records and information security are available in the Cybersecurity Policy (under development), Acceptable Use of Information Technology Facilities Policy and Privacy Policy.

4.22 Staff must only access and use records of the university for legitimate business purposes, with appropriate permissions where necessary.

4.23 Public access to records that are more than 30 years old will be governed by access directions approved by the Director, Governance Support Unit, and made by UTS under the State Records Act.

4.24 Public access to information under the GIPA Act will be managed in line with the university's GIPA delegations and procedures (see Right to information (Staff Connect)).

4.25 Subpoenas, legal warrants or court orders will be managed by UTS Legal Services and must be directed to their attention immediately on receipt.

4.26 Original records must not leave the university's control. Only copies may be provided to external parties on approval (unless originals are required by law).

Using service providers

4.27 Where a service provider creates, captures, uses, stores, retains and/or disposes of records with, or on behalf of, the university, including where service providers host an information system or provide software as a service (SaaS) or cloud storage, the relevant data and/or information systems steward must ensure that:

- UTS retains ownership of records and right of access to its records
- records are captured, stored and managed in line with this policy
- relevant recordkeeping obligations equivalent to the requirements outlined in this policy are imposed on the external party through an enforceable contact, and
- the external party's compliance with recordkeeping obligations in the contract is monitored to ensure the obligations are being met.

Storage of physical records

4.28 Physical records in current use, or on loan from archives, must be stored on campus by the unit responsible for the record.

4.29 Units storing physical records:

- must ensure the records are stored in suitable locations and protected from loss, damage or unauthorised access. Use of storage areas and facilities separate from office areas must be approved by University Records
- are responsible for the recovery of damaged records in the event of a disaster (see Disaster plan for physical records (SharePoint, staff only)).

4.30 Records that are required to be retained but are no longer active or in current use may be transferred to University Records for archives in line with the university's procedures (see Archiving and destroying records (SharePoint, staff only)). Records requiring permanent retention must be transferred as soon as they are no longer in active use.

4.31 UTS may engage a service provider for the ongoing storage of its archived records. Any such arrangements are to be centrally managed by University Records. Units must not engage their own service providers for the storage of their physical records.

4.32 Staff should not hold (store) physical records outside UTS's control. Staff working off campus must comply with recordkeeping practices if they require access to records while off campus.

4.33 The location of physical records must be documented and kept up-to-date.

4.34 All physical records must be handled and stored with care to prevent deterioration, damage or loss.

Records retention and disposal controls

4.35 Records must be retained for the minimum retention periods specified in retention and disposal authorities and normal administrative practice guidelines issued under the State Records Act (refer Schedule 2, State Records Regulation 2015). Any retention requirements specified in other legislation that applies to a business activity, or in a direction from any court or tribunal, statutory body, commission or governing agency, must also be satisfied.

4.36 Records may be kept longer than minimum retention periods if required for ongoing administrative, legal, audit or financial needs of the university, or for historical or research purposes. Longer retention requires consideration of the university's legitimate business needs, resource impacts, public interest and privacy obligations (see Privacy Policy).

4.37 Permanent retention of any record donated to UTS (and not identified as a state archive) will be decided in line with the UTS Archives Collection Guidelines. For significant volumes and/or records with an ongoing resource commitment, the donation must be approved by the Director, Governance Support Unit, or Head, Corporate Information.

4.38 An information system holding records, regardless of whether it is deemed a recordkeeping system or not, must have a retention plan developed and maintained in line with this policy and the university's procedures (see Archiving and destroying records (SharePoint, staff only)).

4.39 The destruction of records, including records held in information systems at UTS or with service providers, or records in information systems pending decommissioning, must be undertaken in line with the university's procedures (see Archiving and destroying records (SharePoint, staff only)).

4.40 The destruction of records and associated recordkeeping metadata requires written authorisation of the:

- head of the relevant unit or data steward where applicable, and
- Head, Corporate Information (or nominated delegate).

4.41 The Head, Corporate Information may issue pre-approved authorisation for certain records to be destroyed locally without formal authorisation. Any such pre-approvals will be in line with the requirements of this policy, and will be documented in the university's procedures (see Archiving and destroying records (SharePoint, staff only)).

4.42 The destruction of any record must be undertaken in a secure manner as appropriate to the format and relevant security classification.

Breaches

4.43 Breaches of this policy and the UTS records management program will be managed under the Code of Conduct and the relevant enterprise agreement.

4.44 A breach of the requirements of the UTS records management program constitutes a breach of this policy.

5. Policy ownership and support

5.1 **Policy owner:** The Deputy Vice-Chancellor (Corporate Services) is responsible for policy enforcement and compliance, general oversight of records, information and privacy management at UTS and oversight of the UTS records management program. The Deputy Vice-Chancellor (Corporate Services) ensures that recordkeeping systems support organisational and public accountability.

5.2 Policy contacts

The Director, Governance Support Unit (GSU) is responsible for implementing this policy and the UTS records management program.

The Director, GSU is also responsible for approving the Information Security Classification Standard (available at Information security (SharePoint, staff only)), which is developed and maintained in consultation with the Chief Information Officer and the Chief Data Officer.

The Head, Corporate Information, on behalf of the Director, GSU, and with the University Records team, coordinates and maintains the UTS records management program, and approves associated procedures and guidelines. This includes:

- publishing and reviewing recordkeeping policies and procedures, standards and guidelines
- assisting new units to implement the records management program
- monitoring the performance of business units against records management standards and procedures and this policy
- providing recordkeeping and Content Manager training and other record-related education programs (including for record contacts)
- providing advice on recordkeeping practices and issues
- coordinating the authorisation of record destruction activities, in accordance with the State Records Act
- managing the UTS archives, including storage of and access to archives held centrally
- administering Content Manager, and
- planning disaster prevention, response and recovery operations relating to records (including the vital records program).

5.3 Others

The senior executive are responsible for ensuring business units under their portfolio follow the requirements of this policy.

Deans, directors and heads of areas must implement the requirements of the UTS records management program for their area of responsibility, and are required to:

- ensure unit records are captured appropriately in a recordkeeping system
- ensure an awareness of recordkeeping requirements
- advocate good recordkeeping practices and sustainable recordkeeping systems
- ensure recordkeeping is addressed in business process procedures
- ensure that all staff under their direction comply with UTS recordkeeping policies and procedures
- comply with contract reporting obligations under the GIPA Act
- schedule and complete records assessment and planning activities
- ensure agreed action plans are supported and implemented, and
- appropriately assign the records contact roles.

All staff must:

- be aware of the UTS records management program and their responsibilities under it
- ensure that records supporting and documenting their business activities are created, captured and protected in line with the provisions of this policy and its procedures, regardless of format
- contact University Records should they require further information or training.

6. Definitions

These definitions apply for this policy and all associated procedures. These are in addition to the definitions outlined in Schedule 1, Student Rules.

Affiliate is defined in the Code of Conduct.

Archives mean records that have continuing value but are no longer required for current use. This includes permanent university and state archives.

Corporate data is defined in the Data Governance Policy.

Data steward is defined in the Data Governance Policy.

Information Security Classification Standard means the official university tool used to assign levels of protection for data and records based on their content. See Information Security Classification Standard available at Information security (SharePoint, staff only).

Information system is defined in the Data Governance Policy.

Information system steward is defined in the Data Governance Policy.

Records means any document or other source of information that is compiled, recorded or stored, in written form, on film, by electronic process, or in any other format or through any other means (as defined under the State Records Act). This includes but is not limited to data (including corporate data) and information held in fields in an information system, documents, emails, folders, messages, chat and posts. Records are considered authoritative or official (also referred to under the State Records Act as a 'State record') where a record is made or received and held by UTS (or held on behalf of UTS by a service provider) in the conduct of its business. Records that are considered unofficial are records that do not provide evidence of, or explain, the functions or activities of UTS, such as copies, reference material, short term facilitative instructions, and some draft documents (excluding legal drafts or drafts used in consultation processes).

Recordkeeping metadata means metadata (data elements captured or used to describe information, such as date created, author, title, etc) required for the appropriate management of records. See Recordkeeping Metadata Standard (PDF, SharePoint, staff only).

Records management program (**the program**) means a university-wide set of procedures and guidelines that enforce the requirements of this policy and the State Records Act.

Recordkeeping system means a subset of an information system that is designed to control information as required by this policy and the State Records Act. The primary recordkeeping system implemented at UTS as part of the records management program is Content Manager (formerly known as TRIM).

State archives means a state record that the State Archives and Records Authority of NSW has control of. A record may be designated as a state archive based on retention and disposal authorities issued under the State Records Act.

Vital records mean records that are essential for the ongoing business of the university, without which UTS could not continue to function effectively or protect its interests. These include, but are not limited to, contracts and associated variations, deeds, memoranda of understanding, licences, evidence of ownership of physical and intellectual property, and other records documenting the legal authority or rights of the university.

7. Approval information

Policy contact	Director, Governance Support Unit
Approval authority	Vice-Chancellor
Review date	2024
File number	UR07/1205
Superseded documents	Records Management Vice-Chancellor's Directive

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	20/12/2017	03/04/2018	New policy.

1.1	Vice-Chancellor	18/03/2020	18/03/2020	Amendments to reflect name change of record keeping system from TRIM to Content Manager, minor changes to retention archiving and disposal controls and additional Staff Connect links.
2.0	Vice-Chancellor	17/05/2021	28/05/2021	Amendments as a result of a scheduled three-year review and to reflect updates resulting from the Policy Impact Project (2020).

Web version

Records Management Policy

References

Acceptable Use of Information Technology Facilities Policy

Code of Conduct

Cybersecurity Policy (under development)

Data Governance Policy

Enterprise agreements

Government Information (Public Access) Act 2009 (NSW) (GIPA Act)

Information Security Classification Standard (available at Information security (SharePoint, staff only))

Information Technology Security Vice-Chancellor's Directive

Guidelines on what constitutes normal administrative practice, Schedule 2, State Records Regulation 2015 (NSW)

Privacy:

- Privacy Policy
- Privacy Management Plan
- Privacy at UTS
- Privacy (Staff Connect)

Records:

- Records and archives
- Records and archives hub (SharePoint, staff only)
- UTS Archives Collection Guidelines

Right to information (GIPA):

- Right to information
- Right to information (Staff Connect)

State Records Act 1988 (NSW)

Sustainability Policy

UTS Delegations