Records Management Policy

1. Purpose

1.1 The purpose of the Records Management Policy (the policy) is to provide 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 (including contractors and contracted bodies) and students.

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 The university recognises that proper creation, capture, management and protection of records supports and enhances the university’s activities, guides decision-making, protects the interests of the university and the public 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, information systems and processes.

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

4. Policy statements

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, are owned by UTS. The university’s ownership of records and right of access to its records must be included in contractual arrangements for outsourced activities.

UTS Records Management Program

4.2 The university 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 must be implemented by all UTS business units.
4.4 Staff must be aware of and participate in the program through the creation, capture, management and protection of full and accurate records documenting the business activities of UTS.

**Recordkeeping systems**

4.5 Records of the university must be captured in a compliant recordkeeping system suitable for the management and protection of the records created and held. For UTS this means:

- the capture and management of digital records in Content Manager (formerly known as TRIM), either directly or as a result of integration or imports
- the registration and management of paper files in Content Manager, or
- an information system which meets recordkeeping requirements for the ongoing management and protection of records held within that system (see also digital recordkeeping in this policy).

**Local record management**

4.6 Recordkeeping systems must be implemented when a business unit is first established, in consultation with University Records, and sustained over the life of the business.

4.7 Recordkeeping requirements are to be embedded in business processes and procedures.

4.8 Business units will monitor their recordkeeping practices through mandatory self-assessments to ensure ongoing compliance and sustainability.

4.9 Business units will 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 faculty/unit level management plan.

4.10 Business units will assign and maintain appropriate administrative support and records contacts roles in line with this policy and the program.

4.11 Where a business unit is being restructured, University Records must be consulted in advance to plan and facilitate the appropriate management of their records.

**File and document management**

4.12 Documents must be captured in a recordkeeping system as soon as practicable to ensure a full and accurate record is stored and managed. This includes but is not limited to correspondence, emails, reports, and file notes detailing verbal decisions and advice.

4.13 Files holding official records must be titled using the UTS File Classification Scheme.

4.14 Minimum metadata is to be captured about records to facilitate the management of those records overtime (see UTS Recordkeeping Metadata Standard (PDF, Staff Connect)).

4.15 The location of paper files and other physical records must be documented and maintained.
4.16 Final documents and records of completed business processes are not to be altered or removed unless in line with the university's procedures on archiving and destroying records (Staff Connect) and/or required by law.

4.17 Original vital records must be lodged with University Records within one month of the document being executed or a final version of the document being approved, as directed by University Records (see vital records program on Staff Connect).

**Digital recordkeeping**

4.18 Where records are held and managed in an information system, the information system steward is responsible for assessing and ensuring compliance with any recordkeeping requirements. Systems must be reassessed for recordkeeping compliance if they undergo major upgrades or changes in functionality or content.

4.19 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.

4.20 Records held in an information system must be retained until the records can be appropriately destroyed, including where systems are being decommissioned or replaced (see also 4.37 to 4.42 for retention, archiving and disposal controls).

4.21 Staff are responsible for ensuring records created or received via personal devices or programs are captured in a university recordkeeping system (see also Acceptable Use of Information Technology Facilities Policy and Privacy Policy).

**Additional requirements for contract management**

4.22 The university will include on its public Register of Contracts details of contracts required to be reported under contract reporting provisions in the Government Information (Public Access) Act 2009 (NSW) (GIPA Act).

4.23 Information required for the Register of Contracts under the GIPA Act must be provided to University Records within one month of a contract’s execution, commencement or variation, in line with procedures issued by University Records (see right to information on Staff Connect).

**Security and access**

4.24 All records (including corporate data) must be allocated one of the four following security classifications:

- UTS Public
- UTS Internal
- UTS Sensitive
- UTS Confidential

These are further outlined and defined in the Information Security Classification Standard (PDF, Staff Connect).

4.25 Records that are classified as UTS Internal, UTS Sensitive or UTS 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 Privacy Policy and Privacy Management Plan and the Data Governance Policy.

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

4.27 Staff may only access and use records for legitimate business purposes, with appropriate permissions where necessary.

4.28 Access to records that are over 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.

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

4.30 Access to information under the GIPA Act will be approved in line with the university’s GIPA delegations and procedures issued by University Records (see right to information on Staff Connect).

4.31 Original records must not leave the university’s control; only copies may be provided to external parties upon approval (unless originals are required by law).

Storage of physical records

4.32 Physical records are to be stored by the responsible business unit or their parent faculty or unit. Non-current records and archives may be transferred to University Records in line with procedures issued by University Records (see archiving and destroying records on Staff Connect).

4.33 Business units storing physical records are responsible to ensure the records are stored in suitable locations and protected.

4.34 Business units storing physical records are responsible for the recovery of damaged records in the event of a disaster (see risk and disaster management for records on Staff Connect).

4.35 Use of storage areas and facilities for storage of physical records must be approved by University Records.

4.36 All physical records must be handled with care to prevent deterioration and damage.

Retention, archiving and disposal controls

4.37 Records must be retained for the minimum retention periods specified in retention and disposal authorities issued under the State Records Act. Any retention requirements specified in other legislation specific to a business activity must also be satisfied, including any restrictions on retention applied to personal information as outlined in the Privacy Policy.
4.38 The destruction of official records and associated recordkeeping metadata requires written authorisation of the:

- relevant data steward or head of area¹, and
- head of University Records (or nominated delegate).

4.39 The destruction of records, including records held in information systems at UTS, or hosted by external contractors or contracted parties, must be undertaken in line with procedures issued by University Records (see archiving and destroying records on Staff Connect).

4.40 Paper documents that have been scanned and recorded in line with procedures (Staff Connect) issued by University Records may be destroyed (as copies only) with approval by the responsible business unit and/or information system owner.

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

4.42 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 must be justified based on resource impacts and privacy considerations and documented (see Privacy Policy).

4.43 Permanent retention of any record not identified as a State archive will be decided in line with the UTS Archives Collection Guidelines as approved by the Director, Governance Support Unit.

**Breaches**

4.44 Breaches of this policy and the UTS Records Management Program will be managed under the Code of Conduct and the relevant enterprise agreement.

4.45 A breach of the requirements of the UTS Records Management Program constitutes a breach of this policy.

**5. Policy ownership and support**

The statements in this section are consistent with the Delegations and are in addition to specific statements outlined in section four of this policy.

**5.1 Policy owner**

The Deputy Vice-Chancellor (Corporate Services) is responsible for general oversight of records, information and privacy management at UTS and the UTS Records Management Program. This role ensures that recordkeeping systems support organisational and public accountability.

¹ Where the business unit or its parent faculty/unit no longer exists or cannot be identified, authorisation will be obtained from the relevant member of the senior executive or the Director, Governance Support Unit.
5.2 Policy contacts

The **Director, Governance Support Unit (GSU)** is responsible for implementing this policy, the UTS Records Management Program and all associated records management procedures and guidelines.

The Director, GSU is also responsible for the Information Security Classification Standard (PDF, Staff Connect), which is developed and maintained in consultation with the **Chief Information Officer** and the **Director, Planning and Quality Unit**.

**University Records (GSU)**, on behalf of the Director, GSU, coordinates and maintains the UTS Records Management Program. This includes:

- developing and reviewing recordkeeping policies and procedures, standards and guidelines
- 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 to business units
- coordinating the authorisation of record destruction activities, in accordance with the **State Records Act**
- managing the storage of and access to archives managed 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 Records Management Program for their area of responsibility, and are required to:

- 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 to 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 and are presented in addition to the definitions outlined in Schedule 1, Student Rules.

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

Authorised users mean staff members who have been delegated the right to access or provide access to a record. This is defined as part of the security classification applied to an individual record or to a group of records.

The following staff members will be considered authorised users where access to certain records is required for the purpose of undertaking their functions:

• the Senior Executive
• UTS Legal Services
• University Records staff or information system administrators
• delegated Right to Information Coordinator, Right to Information Officer(s) or UTS Privacy Officer(s)
• internal auditors undertaking formal audits or investigations (in accordance with the Internal Audit Charter).

Corporate data is defined in the Data Governance Policy.

Data steward is defined in the Data Governance Policy.

File Classification Scheme means the official university tool used to classify records according to university function and broad activity.

Information Security Classification Standard means the official university tool used to assign levels of protection for data and documents based on their content. See Information Security Classification Standard (PDF, Staff Connect).

Information system steward is defined in the Data Governance Policy.

Records mean 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).

There are two subcategories of records at UTS:

• official record means any record made or received and held by UTS (or held on behalf of UTS as part of an outsourced activity) in the conduct of its business.
• unofficial record means records which do not provide evidence of or explain the functions or activities of UTS, such as copies, reference material and short term facilitative instructions, and some draft documents (excluding legal drafts or drafts used in consultation processes).
**Recordkeeping Metadata Standard** means the official university tool that defines metadata required for the appropriate management of records, including documents and data in information systems. See [Recordkeeping Metadata Standard](#) (PDF, Staff Connect).

**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](#).

**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** means 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.

### Approval information

<table>
<thead>
<tr>
<th>Policy contact</th>
<th>Director, Governance Support Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval authority</td>
<td>Vice-Chancellor</td>
</tr>
<tr>
<td>Review date</td>
<td>February 2021</td>
</tr>
<tr>
<td>File number</td>
<td>UR07/1205</td>
</tr>
<tr>
<td>Superseded documents</td>
<td>Records Management Vice-Chancellor’s Directive</td>
</tr>
</tbody>
</table>

### Version history

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved by</th>
<th>Approval date</th>
<th>Effective date</th>
<th>Sections modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Vice-Chancellor</td>
<td>20/12/2017</td>
<td>03/04/2018</td>
<td>New policy.</td>
</tr>
<tr>
<td>1.1</td>
<td>Vice-Chancellor</td>
<td>18/03/2020</td>
<td>18/03/2020</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Web version

[Records Management Policy](#)
References

Acceptable Use of Information Technology Facilities Policy

Code of Conduct

Data Governance Policy

Enterprise agreements

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

Information Security Classification Standard (PDF, Staff Connect)

Information Technology Security Vice-Chancellor’s Directive

Privacy:

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

Records:

- Assessing paper records for scanning (Staff Connect)
- Recordkeeping Metadata Standard (PDF, Staff Connect)
- Records and archives procedures (Staff Connect)
- Recordkeeping at UTS (Staff Connect)
- UTS Archives Collection Guidelines

Right to information (GIPA):

- Right to information at UTS
- Right to information for UTS staff (Staff Connect)

State Records Act 1988 (NSW)