Data Governance Policy

1. Purpose

1.1 The purpose of the Data Governance Policy (the policy) is to:

- establish the principles and practices for the effective management and use of the university's corporate data
- ensure that the university's corporate data is secure and reliable while accessible within a clear system of controls
- ensure that university decision making, planning and reporting is informed by secure, well managed and reliable data, and
- articulate responsibilities for the stewardship of corporate data and information systems supporting the implementation of this policy.

2. Scope

2.1 This policy applies to all staff (including contractors) and students.

2.2 This policy must be adhered to in the collection and management of all corporate data.

2.3 This policy complements the provisions outlined in the following documents, which collectively operationalise data governance for UTS:

- the Privacy Policy, which protects the privacy of all individuals, in particular, personal information
- the Records Management Policy, which outlines the processes for full and accurate record keeping and management
- the Academic Records Policy, which articulates the requirements relating to official academic record documents issued to students and graduates
- the Research Management Policy, which defines the requirements for the management of data resulting from academic research projects at UTS, and
- the Information Technology Security Vice-Chancellor's Directive, which defines the requirements for information system access control and system security.

3. Principles

3.1 Corporate data is a strategic asset of the university. It is governed in line with this policy and stored by approved and appropriate information systems.

3.2 The quality of corporate data should be managed, recognising the importance of high quality data to accurate reporting and evidence-based decision making.

3.3 UTS recognises that effective data governance is dependent on the clear assignment of accountabilities for corporate data and that all corporate data must be actively managed throughout the data lifecycle, from collection to disposal.

3.4 All staff (including contractors) and students are accountable under this policy for the data they collect and manage on behalf of the university.

3.5 The collection and management of personal information (collected as corporate data) should be managed in line with the principles and statements in the Privacy Policy.

3.6 The university acknowledges the use of multiple information systems in the collection and management of corporate data, and the important link between systems governance and data governance.

4. Policy statements

Data management and use

4.1 Corporate data must be secure and reliable, while also accessible for authorised use in accordance with a clear and transparent control framework.

4.2 Accessibility, storage and control frameworks for all corporate data must be developed in accordance with the Privacy Policy and the Information Technology Security Vice-Chancellor's Directive.

4.3 Primary and secondary purposes of corporate data should be clearly understood, applied and communicated in accordance with the Privacy Policy.

4.4 Data quality requirements should be defined in the context of the purpose and use of the data, and necessary data quality monitoring mechanisms put in place.

4.5 Corporate data elements must be defined consistently throughout the university, and definitions made available to all users.

4.6 Disclosure of corporate data to a third party, including for research projects, must be explicitly authorised in accordance with this policy, the Records Management Policy, the Privacy Policy and, where relevant, with the appropriate research ethics clearance (see Research Ethics and Integrity Policy).

4.7 All UTS corporate data will be assigned a security classification in accordance with Records Management Policy.

Data and systems stewardship

4.8 The senior executive in consultation with the Chief Data Officer have overall responsibility for data management planning and improvement for agreed data domains and information systems.

4.9 With regard to corporate data, members of the senior executive and the Chief Data Officer are responsible for:

- assigning data and systems stewards and accountabilities for agreed data domains
- approving allocated security classifications in accordance with the Information Security Classification Standard (PDF, Staff Connect)
- providing resources for the management of data and systems (in accordance with the UTS Delegations)
- resolving any issues escalated from data and/or information system stewards

- prioritising the management and improvement of data governance and associated information systems.

4.10 Data stewards are normally unit directors or senior managers assigned stewardship responsibility for a data domain (or sub-domain) by the Chief Data Officer.

4.11 Data stewards provide detailed oversight of data management, storage, planning and improvement for data within their domain of responsibility, including:

- ensuring that corporate data is appropriately classified in accordance with this policy and the allocated security classifications in accordance with the Information Security Classification Standard (PDF, Staff Connect)
- understanding the policy and legal context for data collection, usage and accessibility (in particular, the Records Management Policy and the Privacy Policy)
- implementing business processes to ensure appropriate data quality and management
- being aware of relevant data flows between systems and setting the conditions for integration of data from different sources
- authorising new data collection and data disposal exercises in accordance with the Privacy Policy and the Records Management Policy
- considering requests for disclosure of corporate data in accordance with this policy and the Privacy Policy
- defining user access and data security requirements for appropriate systems in accordance with the provisions outlined in this policy, the Privacy Policy and the Information Security Classification Standard (PDF, Staff Connect), and
- arranging training for current and potential users before granting systems (and therefore, data) access.

4.12 Other university staff may be assigned the role of information systems stewards. Information systems stewards provide detailed oversight of an information system, and, under the provisions of this policy, are responsible for:

- the management, maintenance and development of the system and its associated procedures
- supporting data quality management initiatives through adoption of relevant technology
- applying appropriate access controls in accordance with the Privacy Policy, this policy and allocated security classifications in accordance with the Information Security Classification Standard (PDF, Staff Connect), and
- ensuring that all privacy requirements (eg privacy notices) outlined in the Privacy Policy and the Privacy Management Plan (PDF) are applied to the management of the information system.

5. Policy ownership and support

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

5.1 **Policy owner**: The **Provost** is responsible for enforcement and compliance of this policy, and ensuring its principles and statements are observed. The Provost is also

responsible for approval of any associated university-level registers and procedures associated with this policy.

5.2 **Policy contact**: The Chief Data Officer is the primary point of contact for advice on implementing and administrating this policy and, in conjunction with the Governance Support Unit, for the consultation and review process. The Chief Data Officer is also responsible for liaising with the Director, Governance Support Unit and the Chief Information Officer to develop and maintain the Information Security Classification Standard (PDF, Staff Connect) (see also Records Management Policy).

5.3 **Others**

Planning and Quality Unit (**PQU**), under direction of the Chief Data Officer, is responsible for:

- managing and maintaining a register (or registers) of data governance roles on behalf of the university
- the development of procedures, management tools and data steward networks to support the implementation of this policy, and
- coordination of educational resources and procedural documents on a dedicated web location.

Information Technology Division (**ITD**), under its Director, is responsible for:

- ensuing the university's IT architecture and information systems operate in line with this and all related university policies (see section 3 in this policy)
- the development of procedures, management tools and information system steward networks to support the implementation of this policy, and
- developing and maintaining a register of information system stewards on behalf of the university.

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.

Corporate data means all data collected by or on behalf of the university or its staff in relation to its normal business activities. Corporate data includes but is not limited to data collection about students, staff, teaching and learning activities, research management, external engagement, web and social media, finance and facilities; but excludes 'research data' as defined in the Research Management Policy.

Data is a collection of facts or statistics that may be used for a particular or unspecified purpose. The format of data and its manner of presentation or collection may vary, depending on the nature of the data.

Data domain means a broad category of corporate data. These domains are specified in the register of data governance roles and may be further specified into sub-domains.

Data element means the smallest named item of data that provides meaningful information (for example, name, address, year, category).

Data lifecycle means the five phases of data management recognised by UTS to achieve strategic and operational objectives and meet legislative requirements:

- **collection** — the creation, acquisition or capture of data
- **storage** — the appropriate retention and organisation of data
- **access** — assuring that authorised users have access to necessary data
- **use** — the appropriate utilisation of data by the appropriate authorised users
- **archive and disposal** — the long-term storage or deletion of data that is no longer required (see the Records Management Policy).

Data quality means an assessment about data's fitness for purpose in a particular context.

Data quality management means the processes in place to manage the accuracy, validity, completeness, consistency and timeliness of data.

Data steward means a senior manager or director with stewardship responsibility for a data domain or sub-domain.

Information systems mean any university system used in the collection, creation, capture or storage of corporate data. This includes but is not limited to databases, business systems, applications, tracking systems, digital records, paper records and recordkeeping systems.

Information systems steward means a senior manager or director with stewardship responsibility for a university information system.

Approval information

Policy contact	Chief Data Officer
Approval authority	Vice-Chancellor
Review date	2021
Version	1.0
File number	UR18/310
Superseded documents	None

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	06/02/2018	03/04/2018	New policy.
1.1	Vice-Chancellor	02/06/2020	02/06/2020	Apply references to the new role and responsibilities of Chief Data Officer.

Web version

Data Governance Policy

References

Academic Records Policy

Information Security Classification Standard (PDF, Staff Connect)

Information Technology Security Vice-Chancellor's Directive

Privacy Management Plan (PDF)

Privacy Policy

Records Management Policy

Research Ethics and Integrity Policy

Research Management Policy

Additional resources

How do I address a data quality issue (Staff Connect)

UTS Data and Information System Stewards Register (Staff Connect)