RECORDS MANAGEMENT PROCEDURES

Category	Governance
Procedure Owner	Group Director Risk and Assurance
Last review	3 April 2023
Next review	3 April 2028
Approval	Vice-Chancellor
Effective date	3 April 2023

1. PURPOSE

The purpose of these procedures is to ensure a clear and consistent approach to the creation, management and Disposal of Information, Data and Records, in a manner which supports both organisational activities and legislative compliance. In particular, these procedures provide guidance and direction on the management of University Data, Information and Records throughout the information lifecycle.

2. SCOPE

These procedures apply to:

- All University Staff and all persons granted access to University Data, Information and Records whether as a result of a partnership, contract or other arrangement; and
- All Information and Records, including metadata, created by or for the University in any format, including but not limited to paper and digital.

3. DEFINITIONS

Data: a general term meaning facts, numbers, letters, and symbols collected and processed to produce information.

Disposal: refers to the transfer of control of or the sale, alteration, destruction or discharge of a Public Record.

Disposal Authority: refers to all relevant Disposal Authorities approved by Archives New Zealand including but not limited to Disposal Authority DA702 for University Public Records.

Executive Sponsor: refers to the University's first point of contact for Archives New Zealand and is currently the Group Director Risk and Assurance.

Information: is created and managed by members of the University community, often in the conduct of the business of the University. Much of the Information created will be evidence of business activity and functions of the University, and therefore, is a Record.

Public Record(s): refers to a University Record that is subject to the requirements of the PRA but excludes academic research data, University special collections, teaching materials and materials created by students are not public records.

PRA:	refers to the Public Records Act 2005 and includes any amendments or replacement statute and secondary legislation.
Record(s):	refers to Information or Data created, received and maintained in pursuance of legal obligations or the business functions and activities of the University.
Staff:	means University employees whether permanent, fixed term or temporary and includes contractors, secondees, interns and others who form part of the University's workforce from time to time or perform some of its activities or functions.
University:	means Auckland University of Technology and includes any entities in which the University has an ownership stake of 50% or more.

4. ACTIONS

The information lifecycle

Information and Records need to be actively managed through each stage of the information lifecycle shown above.

Information governance

Information management activities are guided by the Data and Information Management Roadmap, overseen by the Data and Information Governance Group (DIGG). Minutes from DIGG meetings are available on the pages of the University's intranet (TUIA). DIGG reports activities and progress against the Information Management Roadmap at least annually.

Information and Records creation

University Information and Records must be captured by all Staff and should provide reliable and accurate evidence of business decisions, actions and functions.

Ownership of all Records created or received during the course of University business or activities is vested in the University.

Information and Records storage and archiving

All University Information and Records must be captured in accordance with the University's current Information and Communication Technology Policy and Procedures. These systems support information and Records management processes, and are secure from unauthorised access, damage and misuse.

Records should not be stored or archived in personal email folders, personal drives or external storage media.

To ensure University staff have access to the right information at the right time, all Records stored in an endorsed system for the storage of Records must be captured digitally. It is not necessary to attach paper copies of born-digital Records to official folders.

Born-physical information and Records must be stored in appropriate conditions (i.e. secure, dry and pest proofed). Born-physical Records include paper documents containing physical signatures i.e. signed in ink.

Staff must ensure that Information and Records are left within the custody or control of the University when their employment, secondment or contract ends.

Information and Records use

Staff must only access or use information where this is necessary for a legitimate University purpose.

Whilst information re-use is encouraged, information duplication is discouraged. Staff should collaborate to prevent the storage of duplicate files, wherever possible referring to an organisational single source of truth rather than saving a local copy. The use of organisational templates is encouraged wherever possible.

The University collects and uses personal information about its students, staff and others in order to operate effectively. Personal information held by the University is collected and managed in a responsible, secure manner, in compliance with the Information Privacy Principles outlined in the Privacy Act 2020.

Information and Records sharing

The University's intended approach to information access is one of openness, encouraging appropriate information sharing to improve organisational effectiveness.

Where required by legislative and business requirements, access restrictions are applied to protect personal information; sensitive material; information and Records with restricted access (in accordance with the University's data sensitivity classification). In particular, the University must comply with the Official Information Act 1982 and the Privacy Act 2020 in conducting its activities.

Information and Records disposal

Public Records must be disposed of in accordance with the Disposal Authorities.

The relevant Disposal action for a Public Record is usually either secure destruction of it or archiving and transfer of it to Archives New Zealand (as regulator of the Public Records Act 2005). The appropriate Disposal action for a particular Record is set out in the relevant Disposal Authority.

Disposal must only take place after fulfilling the minimum retention period for that class or sub-class of Records set out in the relevant Disposal Authority. Retention periods in the Disposal Authorities take into account all business, legal and governmental requirements for Public Records.

Disposal guidelines will be issued separately. Please refer to the Executive Sponsor for authorisation to dispose of Public Records in the meantime.

Disposal of other University Records that are not Public Records must take place in accordance with all relevant legal and contractual obligations, or other guidance issued by the University.

Information security

The University demonstrates a commitment to maintaining a robust information security environment, further addressed in the Information and Communication Technology Policy and Procedures.

The default information asset security classification is private. Information assets that have not been specifically classified shall be deemed to be private.

Information integrity

All information and Records management practices in the University are to be in accordance with these Procedures and related policy. Business processes must ensure the maintenance of reliable information and Records.

Organisational information is created, collected, classified, and organised in a manner that ensures its integrity, quality and security. The information asset register records organisational information asset metadata to assist with information asset management, classification, and planning. The register outlines information asset: security, content type, location/source system, information asset steward, information asset administrator, and other related metadata. To access the information asset register, contact the Data & Information Governance Group.

Information and Records management training will be provided for University staff to the level of their responsibility under this policy. Information management resources for Staff are available on TUIA.

Business Continuity plans for each Faculty and Office must include the identification, and means of recovery of, critical information and Records.

5. RESPONSIBILITIES

Staff

Responsibilities of all Staff are to comply with the Records Management Policy and these Procedures.

Managers

Responsibilities of Managers include ensuring:

- Staff reporting to them are aware of, understand and comply with the Policy and procedures;
- All business rules, processes or procedures they are responsible for include information and Records management requirements;
- Staff induction processes include records management responsibilities and expectations;
- When Staff leave the University, they are requested to move any records into the correct systems;
- There is a prompt adjustment of appropriate system permissions when changes to a user's role or status occur; and
- Paper Records are stored in appropriate conditions (i.e. secure, dry and pest proofed).

Business Owners

Responsibilities of Business Owners in relation to the business systems they oversee include ensuring:

- Appropriate access controls and access authorisations are documented and in place to protect information and Records;
- They approve in writing any requests for data feeds from business systems of which they are the Business Owner;
- During any business system commissioning, upgrade, migration or decommissioning the information and Records management requirements are considered and documented;
- Information and Records in business systems adopt and implement the University's information sensitivity classification system;
- Risk assessments for high value or high-risk Records are performed when processes or systems change.

Executive Sponsor

Responsibilities of the Executive Sponsor include:

- Championing and advocating for the implementation of these procedures;
- Reporting to Executive any risks identified with the information management component of these procedures; and
- Regularly reviewing these procedures to ensure the ongoing appropriate management of information and Records.

ICT

Responsibilities of ICT include:

- Ensuring all business systems have an identified Business Owner;
- Liaising with Business Owners and Information and Records Management staff to ensure that University business systems comply with the Policy and these procedures; and
- Liaising with Business Owners and Information and Records Management staff to assess information and Records management in system acquisition, maintenance, upgrades and decommissioning.

Information and Records Management staff

Responsibilities of Information and Records Management staff include:

- providing advice and support to staff on how to comply with the Policy and relevant procedures;
- reviewing and approving in principle disposal of records, subject to final approval from the Business Owner;
- escalating issues regarding non-compliance with the Policy as appropriate; and
- liaising with ICT and Business Owners to ensure that University business systems comply with the Policy.

6. POLICY BASE

Records Management Policy
ICT Policy
ICT Procedures
Privacy Policy
Official Information Policy

Policies and Procedures can be found on **TUIA**.

7. ASSOCIATED DOCUMENTS

Information Sensitivity Classification
Data Governance Framework
UNZ Disposal Authority DA702
What to store where guideline
Research data storage guideline

8. DOCUMENT MANAGEMENT AND CONTROL

Procedure Owner:	Group Director Risk and Assurance
Last review:	3 April 2023
Next review:	3 April 2028
Approved by:	Vice-Chancellor
Effective date:	3 April 2023