THE UNIVERSITY of ADELAIDE

Information Management and Governance Policy

OVERVIEW

The creation and proper management of Information Assets is essential to the success of the University's learning, teaching, research, business and administration activities.

As a publicly funded institution, the University must meet accountability obligations and Information Assets provide evidence of its activities and decision-making to external regulators, internal and external auditors, accreditation and funding bodies. In addition, the University needs to provide the public with access to Records under Freedom of Information and for legitimate research purposes.

The maintenance and retention of certain Information Assets also form an "institutional memory", documenting over time the University's history, organisation, operations, research activities and outputs as well as other contributions to the wider community.

University Information Assets are the property of the University and not of the Personnel who create them, or to whom they are entrusted.

This Policy affirms the University's duty to comply with mandatory laws and best practice codes relating to Information Management (including the *State Records Act 1997* and the *Australian Code for the Responsible Conduct of Research* (2018)) and articulates the responsibilities of all Personnel with respect to the creation, maintenance, Disposal and accessibility of Information Assets.

SCOPE AND APPLICATION

This Policy applies to all Information Assets throughout the management of the Information Lifecycle and includes Information, Data or Records, in any format, where it is created or received through the conduct of University business.

Research Data created in the course of any research activity hosted by the University is also considered an Information Asset and is subject to this Policy, while taking into account any third party agreements, relevant contractual arrangements and the related *Research Data and Primary Materials Policy* which further stipulates ownership and responsibility related issues regarding Research Data.

This Policy applies to all Personnel who create or receive Information Assets on behalf of the University or in the course of their University affiliation. This Policy also applies to the management of Information Assets of University Controlled Entities.

This Policy must be read in conjunction with the Information Management and Governance Framework.

POLICY PRINCIPLES

1. **The University proactively manages its Information as business-critical and strategic assets**

   Information is regarded as a vital asset of the University: its value, both current and future, is determined, understood, governed and leveraged to document and support business decisions and outcomes and meet statutory obligations.

   - All University Information Assets will be managed throughout the Information Lifecycle in accordance with the Information Management and Governance Framework.
   - Information Assets of high value or high risk will be maintained and must not be destroyed without proper authorisation in accordance with the Information Management and Governance Framework.
   - Information Assets (administrative, legal, financial or informational) of enduring value and significance will be maintained by the University Archives program.

2. **The University ensures responsibility for managing Information Assets is clearly assigned and documented**

   - All University Information Assets must be allocated an Information Steward by the appropriate Information Domain Custodian as outlined in the Information Management and Governance Framework.

3. **The University manages its Information Assets to meet compliance and accountability obligations and mitigate risk**

   The University determines and documents what Information Assets need to be created and kept in accordance with compliance requirements and a risk management approach to support business objectives and satisfy stakeholder expectations and interests.

   - Information management guidelines, policies and procedures will be established, maintained, and detailed in the Information Management and Governance Framework. This includes record keeping and Disposal procedures, Information classification and security guidelines and standards.
   - Information management guidelines, policies and procedures will be designed to support the compliance with Records and Information Management requirements in laws, regulations, contracts and agreements applicable to its operations. Legal and legislative compliance responsibilities are detailed in the Information Management and Governance Framework.

4. **The University relies on its Information Assets to document, support and substantiate business decisions, outputs, and outcomes**

   Information Assets are captured and stored effectively so that they are accurate, complete, reliable, re-usable and irrefutable for business, evidentiary, research, compliance and reporting purposes.

   - Information Assets and related metadata must be captured in University-approved and supported storage per guidance provided to staff and students.
   - Once created and captured, University Information Assets may not be altered and can only be destroyed in accordance with the University Disposal Schedules.

5. **The University maintains a robust Information security environment**

   - Information Assets and Data must be clearly identified and classified by the Information Steward as detailed in the Information Classification and Protection Standard.
   - Based on the classification, University will apply consistent security controls at a level commensurate with the values of the Information and impact on University in the event that the security of the Information is compromised.

6. **The University is committed to the responsible collection, retention and handling of confidential, personal and sensitive Information.**

   Information Assets are managed and held within a secure environment that makes them easy to find as well as appropriately accessible and shared (subject to access, ethics, privacy, confidentiality and contractual requirements).

   - Collection, use, disclosure and management of, and provision of access to Information Assets that is personal Information (including sensitive personal Information) or Data is subject to the University Privacy Policy and Privacy Management Plan https://www.adelaide.edu.au/policies/62/.

AUTHORITIES

Key	*Authority Category*	*Authority*	*Delegation Holder*	*Limits*
University Operations	Information Management	Disposing of University records	University Librarian	
University Operations	Legal Compliance	Responding to South Australia Police (SAPOL) requests, warrants and subpoenas on the University's behalf, excluding routine communications between Security and SAPOL, including requests supported by a Tasking Number, or Policy Incident Report	General Counsel	
University Operations	Information Management	Granting of access to University records under the *Freedom of Information Act 1991*	Freedom of Information Officers	
University Operations	Information Management	Compliance with the *State Records Act 1997*	Vice-Chancellor and President	

ROLES AND RESPONSIBILITIES

1. Information Management and Data Governance

1.1. Each Information Domain (e.g. Student Management, Human Resources, External Engagement) must have a designated Information Domain Custodian and, one or more Information Stewards. These roles and associated responsibilities are detailed in the Information Management and Governance Framework.

1.2. All Personnel must, in the conduct of operational, academic and research activity:

a) comply with Information Management processes, practices and requirements in accordance with this Policy and the Information Management and Governance Framework. Local area procedures and regulatory environments may also apply

b) cooperate and assist with Information Management monitoring, analysis and review of processes to ensure Information assets are being created, captured and managed.

1.3. All Personnel must complete induction and training on Information Management tasks and responsibilities as required.

2. Managing Information Assets

2.1 All Personnel, in the performance of their University duties, must create, manage, store, access, use and dispose of Information Assets in accordance with this Policy and procedures, guidelines and policies and guidelines outlined in the Information Management and Governance Framework. Local area procedures, and ethics, contractual and/or regulatory requirements may also apply.

2.2 All Personnel must manage Information Assets digitally unless there are specific, legal, safety or practical reasons for keeping physical Information Assets.

2.3 All Personnel must act on and report suspected and actual breaches of Information Assets in accordance with the University's Data Breach Response Plan.

DEFINITIONS

Data

Factual Information (such as measurements or statistics) used as a basis for reasoning, discussion or calculation. **Research Data** is specifically defined in the *Research Data and Primary Materials Policy.*

Disposal

Umbrella term for the ultimate fate of an Information Asset, which could be that it is kept permanently or destroyed after a defined period of time. The State Records Act requires the University to dispose of its Information Assets in accordance with approved Disposal Schedules

Disposal Schedule

Sets out the legally mandated minimum amount of time specific types of Information Assets must be kept

Information

Codified knowledge, which is transferred and stored by written or electronic means

Information Asset

Information, Data and Records, in any format, where it is created or received through the conduct of University business and treated as an asset and resource that the University harnesses to meet its strategic, operational and legal needs. May include, but not limited to: written or electronic documents, Records, publications, webpages, emails, text messages, spreadsheets, photographs and images, databases, tools and applications, drawings, plans, sound and video recordings, etc

Information Domain

Broad Category within which University of Adelaide Information and Data can be identified and managed. Examples of Information Domains: student Data, finance Data, human resources Data etc.

Information Sub-Domain

Specific groups of Information that is related to an Information Domain. Examples of Information Sub-Domains: Enrolment, General Ledger, Talent Acquisition, Research Project etc

Information Domain Custodian

Responsible owner for one or more Information Domains area in full.

Information Governance

Information Governance is the specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and disposal of Information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of Information in enabling an organization to achieve its goals (Gartner definition).

Information Lifecycle

Includes planning and designing for Information, creating or receiving Information, storing and sharing Information, maintaining and managing Information, applying and using Information to accomplish goals and meet business needs, and disposing of the Information (which may include destruction or transfer to archives for ongoing retention)

Information Management

The structures, systems, people and processes to capture, manage, preserve, store and deliver the right Information to the right people at the right time regardless of location. Information is delivered through multiple channels and interfaces. It is managed throughout the Information Lifecycle regardless of its source or format

Information Security

The preservation of the confidentiality, integrity and availability of Information

Information Steward

Responsible for the quality, integrity and ethical use of Information within one or more Information sub-domains on a day-to-day basis.

Personnel

For the purposes of this policy means people associated with the teaching, learning, research, enabling and supporting activities of the University and includes:

- University officers appointed under the *University of Adelaide Act 1971* and external members of the governing body or any committee of the University of Adelaide Council
- academic and professional staff
- titleholders, adjuncts, academic visitors and affiliates of the University
- researchers (including HDR students)
- contractors, consultants, and volunteers

Record

Recorded Information or Data in any form that is created or received by the University in the conduct of its affairs, transaction of its business functions or resulting from research activities and retained as evidence of that activity. This incorporates both hardcopy and digital Records, including electronic Records held in email systems, business systems and digital repositories

Records Services File No.	2018/11763
Policy Custodian	Chief Operating Officer
Responsible Policy Officer	Chief Data & Analytics Officer
Endorsed by	Vice-Chancellor's Executive on 29 May 2024
Approved by	Vice-Chancellor and President on 5 August 2024
Related Documents and Policies	Information Management and Governance Framework Cyber Security Framework Records Management procedure (to be finalised) Contracts and Agreements Policy Data Breach Response Plan Freedom of Information Policy IT Acceptable Use and Security Policy IT Security Procedures Responsible Conduct of Research Policy and Procedure Open Access Policy Privacy Policy Research Data and Primary Materials Policy Information Classification and Protection Standard Risk Management policy
Related Legislation	*State Records Act 1997*
Superseded Policies	*Information Management Policy*
Effective From	5 August 2024
Review Date	4 August 2027
Contact for Queries about the Policy	Chief Data & Analytics Officer, Dan McHolm, 831 **36300** dan.mcholm@adelaide.edu.au