THE UNIVERSITY of ADELAIDE

Information Management 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. The University's *Research Data and Primary Materials Policy* further stipulates ownership-related issues regarding Research Data.

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.

This Policy also embodies best practice Information Management standards of both the state and federal government's records authorities as well as the Australian Standard *AS ISO 15489 (2017): Records Management*.

SCOPE AND APPLICATION

This Policy applies to all Information Assets throughout the management of the Information Lifecycle and includes any information or record, 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.*

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 of Adelaide Controlled Entities.

This Policy must be read in conjunction with the *Information Management Procedure Manual*.

This Policy also inter-relates with the University's *Contracts and Agreements Policy, Risk Policy, Privacy Policy* and *Freedom of Information Policy.*

POLICY PRINCIPLES

1. **The University has a fundamental obligation to proactively manage its information as business-critical 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.

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

   Executive and senior management must assign responsibility for Information Assets to designated staff to ensure they are managed for the best outcomes of the University, its Personnel, students, partners, affiliates and the broader community.

3. **The University creates and retains its Information Assets to meet 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.

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

5. **The University effectively balances the disclosure of Information Assets with the need to maintain confidentiality as required**

   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).

AUTHORITIES

Key	*Authority Category*	*Authority*	*Delegation Holder*	*Limits*
University Operations	Information Management	Implementing and monitoring Information Management standards	University Archivist & Manager, Special Collections Archives and Recordkeeping (SpARK)	
University Operations	Information Management	Disposing of University records	University Archivist & Manager, Special Collections Archives and Recordkeeping (SpARK)	

Key	*Authority Category*	*Authority*	*Delegation Holder*	*Limits*
University Operations	Legal Compliance	Responding to South Australia Police (SAPOL) requests, warrants and subpoenas on the University's behalf, including any response to a warrant or subpoena and copies of CCTV footage, but excluding routine communications between Security and SAPOL, including requests supported by a Tasking Number, or Policy Incident Report	General Counsel and Executive Director, Legal and Risk	
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	

PROCEDURES AND RESPONSIBILITIES

1. Information Management Governance

1.1 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 Procedure Manual*. Local area procedures and regulatory environments may also apply

b) cooperate and assist with Information Management monitoring and audits of local areas.

1.2 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 the *Information Management Procedure Manual.* 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.

3 Information Management Responsibilities

3.1 In addition, the following have specific responsibilities as outlined below:

	RESPONSIBILITY
University Personnel that are Researchers	• Ensure a formal agreement with a Researcher's new institution affirming an intention to curate Information Assets is in place. • Proactively publish research Information Assets in line with the Open Access Policy of the University and those of relevant funding bodies (eg Australian Research Council and National Health and Medical Research Council), contractual or other obligations and in line with the *Australian Code for the Responsible Conduct of Research*.
University Personnel assigned as Information Custodians	• Contribute to the development of any necessary local area Information Management instructions or guidelines, consistent with this Policy and the *Information Management Procedure Manual*. • Contribute to reporting activities for local area Business Systems and Information Management practices relevant to their assigned Information Assets. • Keep Heads of School/Branch and Executive Managers informed of any issues regarding their Information Assets and contribute to assessing risks to Information Assets assigned to them throughout their lifecycle. • Contribute to business process analysis and mapping of their local area to identify Information Management inefficiencies and solutions. • Promote Information Asset quality awareness, requirements, analysis, metrics and business rules for their local area. • Locate authoritative Information Assets for which they are responsible to assist others in their business and research activities. • Contribute to useability testing for new Business Systems and Information Management practices of their local area.

	RESPONSIBILITY
Business System Administrators	• Manage Business Systems that support the University in fulfilling its business, operational, academic and research objectives. • Consult with the University Archivist and Manager, SpARK when designing and/or implementing Business Systems. • Ensure adequate Information Management functionality within Business Systems or integration with the University's dedicated Electronic Recordkeeping System in order to effectively capture, identify, store, use, protect, preserve and dispose of Information Assets. • Ensure Information Assets can be captured once, where possible, but reused as needed as a reliable source of truth. • Report periodically on the effectiveness and reliability of Business Systems in managing and storing Information Assets. • Ensure Information Assets are accessible for as long as required and if necessary preserved within Business Systems. • Consult with the University Archivist and Manager, SpARK when a Business System is near end of life and archive or migrate digital Information Assets when Business Systems, software and/or media are upgraded or decommissioned.
Heads of School/Branch	• Foster, at the local level, an organisational culture that values and manages information as assets and enablers for University business. • Develop local area Information Management processes and guidelines as needed and consistent with this Policy and the *Information Management Procedure Manual.* • Ensure Personnel are inducted and trained in their Information Management responsibilities. • Assign relevant Personnel as Information Custodian/s to manage and curate local area Information Assets. • Provide approval for the disposal of information assets in accordance with the University's disposal regime and in consultation with the University Archivist and Manager, Special Collections, Archives and Recordkeeping. • Endorse the permanent removal of Information Assets from University custody or control. • Manage access to University Business Systems as authorised by the IT Acceptable Use and Security Policy. • Take immediate action to contain suspected or actual breaches of Information Assets in accordance with the University's Data Breach Response Plan.
University Archivist and Manager, Special Collections, Archives and Recordkeeping (SpARK)	• Develop and maintain the *Information Management Procedure Manual*. • Establish and maintain an audit regime for Information Management. • Report to the Information Management Governance Committee on Information Management performance and compliance. • Provide or contribute to Information Management induction, support and training of Personnel. • Assess the business risks associated with managing Information Assets in accordance with the University Risk Policy. • Maintain a Disposal regime for Information Assets in accordance with legislative and compliance requirements. • Maintain the University Archives to support the ongoing retention, preservation and accessibility of permanent value Information Assets. • Administer and upgrade as necessary the University's dedicated Electronic Recordkeeping System. • Administer public access to archival Information Assets within the constraints of security, confidentiality, privacy, contractual obligations, ethical considerations and archival access conditions. • Authorise permanent removal of Information Assets from University custody or control on the endorsement of a Head of School/Branch or Executive Manager.
Executive Deans and Divisional Heads	• Ensure that adequate resources are available to implement this Policy and the *Information Management Procedure Manual*. • Address business risks associated with managing Information Assets in accordance with the University Risk Policy.

	RESPONSIBILITY
Information Management Governance Committee	• Oversee the University's Information Management governance framework. • Advise the University Archivist and Manager, SpARK on Information Management strategy, procedures and operations. • Receive regular reports from the University Archivist and Manager, SpARK on Information Management performance and compliance. • Report Information Management matters to the Vice-Chancellor Executive Group as required.

DEFINITIONS

Access

Right, opportunity, means of finding, using or retrieving information

Business System

A combination of hardware, computer software, business rules and planning which together allows the University to carry out specific jobs, manage aspects of its business, and maintain a level of quality and efficiency. A Business System may be a single computer program, or may be several linked programs, which form the underlying infrastructure of the University. Examples of a Business System include financial and HR systems such as PeopleSoft, research management systems such as ResearchMaster, and client management systems such as CRM

Business System Administrator

Means the University staff member or area responsible for the administration of a University Business System

Controlled Entity

Has the same meaning as in the University's Controlled Entity Policy

Data

Factual information (such as measurements or statistics) used as a basis for reasoning, discussion or calculation

Disposal

In an Information Management context, Disposal is an 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

Electronic Recordkeeping System

An automated system used to manage the creation, use, management, storage and disposal of physical and digital Information Assets, maintain appropriate contextual information (metadata) and links between Information Assets to support their value as evidence

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 Custodian

University Personnel with ultimate accountability for the management of local area Information Asset/s assigned to them by their Head of School/Branch or Executive Manager

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

Metadata

Data describing context, content and structure of Information Assets and their management through time. Metadata in a business or recordkeeping system is required for uniquely identifying Information Assets, authentication, capturing content, structure and context, administering access and disposal terms and conditions, tracking and documenting use history, enabling discovery, retrieval and delivery of Information Assets to authorised users and restricting unauthorised use

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 and consultants
- 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

Research Data

As defined in the *Research Data and Primary Materials Policy*, data are facts, observations or experiences on which an argument, theory or test is based. Data may be numerical, descriptive or visual. Data may be raw or analysed, experimental or observational. Data includes: laboratory notebooks, field notebooks, primary research data, questionnaires, audiotapes, videotapes, models, photographs, films, test responses. Research collections may include slides, artefacts, specimens, samples. Provenance information about the data might also be included: the how, when, where it was collected and with what (for example, instrument). The software code used to generate, annotate or analyse the data may also be included

Researcher

A staff member, student, affiliate or titleholder of the University of Adelaide who is involved in the conduct of research associated with the University anywhere in the world

Records Services File No.	2018/11763
Policy Custodian	Deputy Vice-Chancellor and Vice-President (Academic)
Responsible Policy Officer	University Librarian
Endorsed by	Academic Board Out of Session Committee on 25 November 2020
Approved by	Vice-Chancellor and President on 26 November 2020
Related Documents and Policies	*Contracts and Agreements Policy* *Copyright Compliance Policy* *Data Breach Response Plan* *Freedom of Information Policy* *Information Classification and Protection Guideline* *Information Management Handbook (TBA)* *Information Management Strategy (TBA)* *IT Acceptable Use and Security Policy* *IT Security Procedures* *Open Access Policy* *Privacy Policy* *Research Data and Primary Materials Policy* *Responsible Conduct of Research Policy* *Risk Policy* *Strategic Plan: Future Making – A 21st Century University for Adelaide*

Related Legislation	*State Records Act 1997*
Superseded Policies	*University Records Policy*
Effective From	26 November 2020
Review Date	26 November 2023
Contact for Queries about the Policy	Siân Woolcock, University Librarian, 8313 5700, sian.woolcock@adelaide.edu.au.