Standard

Records and Information Management

Overview

This standard, in conjunction with the Records and Information Management Policy, provides operational advice and guidance for the effective management of physical and electronic records and information, collectively known as information assets.

Information assets can be in physical form such as a letter or a hardcopy file containing various documents but are most commonly in electronic form. Electronic information assets encompass information in all University business systems. This includes the records management system, Content Manager, as well as everything from email, Teams, SharePoint, network drives, student management systems, Workday, ServiceOne, and more.

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. As a publicly funded institution, the University needs to provide access to records under the Freedom of Information framework as well as other legislative and research purposes.

The maintenance and retention of certain information assets also form an institutional memory. This documents the University's history, organisation, operations, research activities, outputs, and other contributions to the wider community.

University information assets are the property of the University and not of the staff who create them, or to whom they are entrusted. The University's Research Data Management Procedures further stipulates ownership-related issues regarding Research Data.

This standard will provide an overview of the lifecycle management of information assets across the University and will be supported by a more detailed reference guide to be created in conjunction with every business system owner.

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 standard, while taking into account any third-party agreements, relevant contractual arrangements and the related Research Data Management Procedures.

This standard applies to the management of information assets across the University, including Flinders University Controlled Entities. The University will also ensure it has processes in place for engaging with third party providers who manage information assets on our behalf, in particular those that are sensitive or contain personal information.

APPROVED 22 April 2025

Contents

Disposal Programs

Flinders University keeps information assets for the legislated period as defined in various General Disposal Schedules (GDS) approved by State Records Council. Some of the schedules applicable to Flinders University include:

- GDS 21v5 - Digitisation of hardcopy records
- GDS 24v5 - South Australian Universities
- GDS 30v2 - State Government Agencies
- GDS 47 - Records of relevance to allegations of Child Abuse matters

These schedules divide information assets into various categories based on their function, activity, and class. Some examples are provided below:

Function	Activity	Class	Retention
Finance Management	Grants	Successful grant applications	Destroy after 8 years
Human Resources	Appointment	Unsuccessful applications	Destroy after 1 year
Learning and Teaching	Curriculum Development	Development of curricula including proposals and reports	Retain Permanently
Research	Intellectual Property	Infringements of University Intellectual Property	Destroy after 10 years
Student Administration	Academic Progress	Practicum assessment documentation for professional accreditation	Destroy after 25 years

Most information assets should be managed through their lifecycle in the originating business system, where possible. Where information is required to be managed outside the originating business system the following should be applied:

Retention Period	Management of information asset
Less than or equal to 5 years	Lifecycle managed in originating business system
6 years or more	Lifecycle managed in Content Manager
Permanent Value	Move to Content Manager for transfer to State Records

Disposal programs should be run regularly by business system owners and, at a minimum, run every 12 months. This will ensure the University is not keeping personal identifying information, personal health information, or other information longer than required. Running regular disposal programs provides the following benefits:

Reduced Cybersecurity Risk	**Security of Data** - regular disposal ensures sensitive information is permanently removed, reducing the risk of data breaches. **Mitigate Vulnerabilities** - eliminate outdated files that may contain superseded information, security flaws, or sensitive data.
Cost Savings	**Storage Overhead** - clearing unnecessary data reduces storage costs, freeing up space on servers and cloud platforms.
Improved Search Results	**Precision** - remove obsolete files from search indexes, ensuring relevant results for system users. **Enhanced User Experience** - faster search results lead to improved productivity.

Approved Systems

Under GDS 21, an approved system is a records management system or other business system that has been certified to accept digitised renditions of an original hard copy document as the official record. The hard copy document can be destroyed, and the digitised renditions are then treated as the official record under the State Records Act 1997 and must be retained for the minimum period required under the appropriate disposal schedule.

Approved systems within Flinders University contain the necessary metadata elements together with staff having sufficient knowledge to accurately capture digital renditions of their hardcopy documents. An approved system requires three elements:

1. The system contains the metadata elements listed in the Information Asset Metadata Standard.
2. Staff using the system have read, understood, and follow the Information Assets Digitisation and Preservation Standard.
3. The system owner has applied for and received approval to digitise, capture, then dispose of their hardcopy documents from the Director of Library Services (or delegate).

With these three things in place, hardcopy records can be digitised and destroyed[1] once the electronic item is stored in the system. Systems can be approved for GDS21 certification for everyday use of digitising hardcopy documents, or for once-off backlog digitisation projects.

Approved systems must be reevaluated after every major upgrade to ensure continued compliance. This ensures that the appropriate metadata is created and maintained, digital records can be relied upon as evidence, records cannot be altered, and that appropriate controls are in place governing security, access, and disposal.

Current Approved Systems

Content Manager 23.4

[1] Destruction of all hardcopy source documents with a temporary retention value and permanent retention documents created after 1 January 2005. See GDS 21v5 for the full list of exclusions.

Information Classification

Where applicable, information should be classified in business systems based on its sensitivity, confidentiality, and regulatory requirements. Refer to the University's Information Classification and Handling Procedures for further detail on classifying and securely storing information assets.

Version Control

Business systems that store electronic documents must establish procedures for version control to ensure that the most current and accurate information is being used. New versions of documents are to be created where there is a major update, for example, updated policy document. Smaller, incremental changes can be managed effectively using new revisions rather than versioning. Documents should include naming conventions, revision tracking, and approval processes for updates. Refer to the University's general Naming Conventions for Digital Documents. This is a guide only and each business area can establish their own naming conventions. Where possible try to follow these key rules:

- Avoid using non-alphanumeric characters in titling
- Title with the most static information first through to your most changeable information at the end. For example;
  - Portfolio working group - Agenda - 12 January 2024
  - Portfolio working group - Minutes - 19 January 2024
  - Portfolio working group - Action Items Update - 9 February 2024

Training and Awareness

The Records and Information Management Policy requires all staff to obtain and maintain sufficient skills and knowledge to manage information assets within their area of responsibility. The University provides training programs and resources to assist staff with information management best practices, policies, and guidelines. Staff must work through the information management training that is provided as part of the onboarding process as well as seeking out further training and information on the Flinders University website.