Information Management Policy

1. COMPLIANCE OBLIGATION SUPPORTED

State Records Act (WA) 2000

2. PURPOSE

To establish the framework and principles for effective data and information management that supports the business functions and activities of Curtin University.

3. POLICY STATEMENT

3.1. The University will establish and maintain data and information management practices that result in appropriate and ongoing management of these assets to support decision making, fulfil compliance obligations, demonstrate accountability, reduce risk, progress Curtin's strategic priorities and meet stakeholder expectations.

3.2. Management of University data and information will be based upon the following principles:

3.2.1. The University will recognise data and information as a valuable asset that supports University functions and activities

3.2.2. Data and information created or received during the course of Curtin activities, including Curtin activities contracted out to third parties, is vested in the University and remains under University control unless:

a) There is a written agreement in place between the University and the other party stating that the data and information is owned by other parties, or;

b) The data or information constitutes Intellectual Property that is vested in an individual or community as per the University's *Intellectual Property Policy*.

3.2.3. Data and information will be discoverable and reliable through:

a) Managing data and information throughout its lifecycle

b) Appropriate creation, capture, classification, organisation, storage, retention and disposal of data and information

c) Practices and systems that support the integrity, findability and trustworthiness of data and information

d) Practices and systems that support the right data and information being available to those authorised to access it when they need it in accessible formats consistent with the principles of Universal Design.

3.2.4. The University will protect and secure data and information from unauthorised access, alteration, deletion or misuse. This includes:

a) Assigning the following Information Security Classifications to our data and information:
- Public
- Internal
- Sensitive
  - Sensitive – Legal
  - Sensitive – Personal
- Restricted
  - Restricted - Personal

b) Managing data and information in accordance with its Information Security Classification and/or in accordance with contractual obligations should they specify handling requirements.

c) Taking steps to meet privacy and responsible handling obligations with regards to the collection, use, storage, access to and disposal of data and information.

d) Adhering to contractual obligations with regards to the management of data and information that sits outside of our Information Security Classifications, such as data and information from government agencies which require the application of the Australian Government's Protective Security Policy Framework (PSPF) for data and information assessed as Security Classified.

3.2.5. The University will retain and dispose of data and information in accordance with the applicable Retention and Disposal Authorities, legal requirements, business need and risk appetite.

3.2.6. Responsibilities and accountabilities are outlined in the *Information Management Procedures*.

4. SCOPE OF POLICY

This policy applies to the University Community, including Council members, students, staff, University Associates, Curtin controlled entities, and all persons participating in University business or activities, including whether as a visitor, adjunct appointee, service provider, contractor or volunteer who manages Curtin data and information.

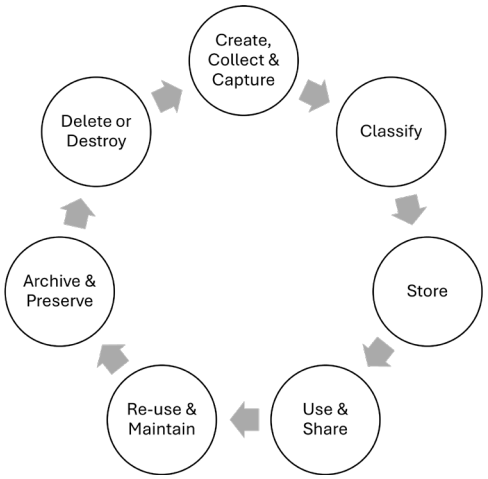
5. DEFINITIONS

(Note: Commonly defined terms are located in the *Curtin Common Definitions*. Any defined terms below are specific to this document)

Data
Facts, figures, observations and experiences that are collected for analysis, reference, decision-making and to gain knowledge. Data acts as the building blocks for information and knowledge. This definition includes Research Data, Confidential Data and Sensitive Data as defined in the *Research Data and Primary Materials Policy*.

Information
Any communication or representation of knowledge such as facts, data or opinions in any medium or form. This definition includes, but is not limited to, documents, emails, webpages, images, audio visual files, social media posts, chat messages, building plans and other types of knowledge captured in digital or hard copy format.

Information Lifecycle
The stages through which information passes, from creation or collection through to destruction, deletion or Archival preservation. Stages include Creation, collection and capture; Classification; Storage; Use and sharing; Reusing and maintaining; Archiving and preserving; Deleting and destroying.



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.

Retention and Disposal Authority
A legal instrument which:

- sets the minimum retention period that different categories of data and information must be held before their legal disposal
- authorises the destruction of data and information that have reached their minimum retention period
- identifies data and information that will be retained permanently as State or University Archives.

Universal Design
As defined in the Disability Inclusion Policy - The design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialised design (and otherwise as defined by Dr. Sheryl Burgstahler, University of Washington (Universal Design of Instruction (UDI): Definition, Principles, Guidelines and Examples).

6. SUPPORTING PROCEDURES

Disclosure of Personal Information Procedures
Information Management Procedures

7. RELATED DOCUMENTS/LINKS

Internal

- *Accessible Information Procedures*
- *Cyber Security & Information and Communication Technology (ICT) Appropriate Use Policy*
- *Information and Communication Technology (ICT) Appropriate Use Procedures*
- *Information Breach Policy*
- Information Security Classifications Summary Table
- Information Security Classification Toolkit
- *Intellectual Property Policy*
- *Privacy Policy*
- *Research Data and Primary Materials Policy*
- Retention and Disposal Authorities

External

- Australian/International Standard ISO/AS 15489: Records Management
- Australian government Protective Security Policy Framework (PSPF)
- *Australian Privacy Principles*
- *Electronic Transactions Act 2011 (WA)*
- *Evidence Act 1906 (WA)*
- *Freedom of Information Act 1992 (WA)*
- *Higher Education Standards Framework (HESF): Standards 2.1.2 & 7.3.3*
- *Information Management Framework for Western Australia*
- *State Records Act 2000 (WA)Privacy Act 1988 (Cth)*
- *Privacy and Responsible Information Sharing Act (WA)*
- *Public Sector Management Act 1994 (WA)*
- *Security of Critical Infrastructure Act 2018 (Cth)*

Policy Compliance Officer	Krista Bell, Director, Data and Information Governance

Policy Manager	Chief Operating Officer
Approval Authority	Senior Executive Team
Review Date	1st April 2031

REVISION HISTORY (*filled out by Risk, Compliance and Audit*)

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
New	Approved	01/04/2008	Planning and Management Committee	PMC 24/08	Attachment 1 to Document No 00334/08
	Administratively Updated	16/10/2012	Director, Legal and Compliance Services		Policy Contact Updated
	Amended	26/11/2013	Planning and Management Committee	PM 94/13	Attachment 2 to Document No 01256/13 (previously Recordkeeping Policy)
	Administratively Updated	06/10/2015	Director, Legal and Compliance Services	EC 76/15	Executive Manager Title Changes
	Approved	02/11/2017	Planning and Management Committee	PMC 87/17	Attachment A to Item 12
	Approved	05/02/2026	Senior Executive Team	SET 03/2026	Attachment A to Item 2.1