Information Management Procedures

1. COMPLIANCE OBLIGATION SUPPORTED

Information Management Policy

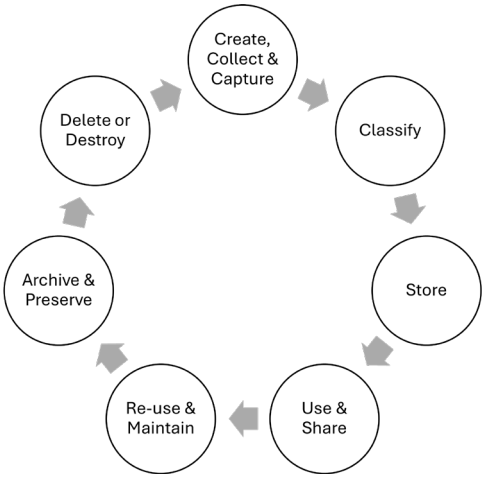
2. PROCEDURAL DETAILS

This document outlines the procedures for managing data and information created, collected or used for undertaking research, teaching and learning activities, as well as engagement, administrative and commercial activities. It applies to data and information regardless of format.

2.1 The Information Lifecycle

Data and information requires effective management throughout the information lifecycle to ensure its authenticity, integrity, reliability, accessibility, useability and security is maintained and that it is used for the purposes intended.

Information must be protected from loss, theft, unauthorised access or destruction, while being available to those who are authorised to access it, by ensuring it is appropriately created, stored, classified, protected, disposed of or retained.



3. RESPONSIBILITIES

The following responsibilities apply to all individuals, and where specified, Areas, regardless of location or role:

3.1 Individuals are to comply with any restrictions or obligations with regards to the management of data and information as required by:

a) any legislative requirements to release information (including to regulators)
b) any compliance and contractual requirements related to the data and information
c) the Information Security Classification category assigned to the information
d) relevant Policies and Procedures including, but not limited to the:
- *Accessible Information Procedures*
- *Disclosure of Personal Information Procedures*
- *Diversity, Inclusion and Belonging Policy*
- *Cyber Security & Information & Communication (ICT) Appropriate Use Policy*
- *Information and Communication Technology Appropriate Use Procedures*
- *Privacy Policy* and the *Privacy Procedures*

3.2 CREATE, COLLECT AND CAPTURE

a) Individuals will create data and information in the course of undertaking teaching, learning, research, engagement, administrative and commercial activities that supports those activities.

b) Individuals will consider accessibility, diversity and inclusion at the point of creation of data and information to ensure that appropriate language and formats are used.

c) Individuals will only collect the minimum amount of Personal Information necessary from students, research participants, community members and others to undertake the relevant University activity for which they are collecting the information.

d) Data and information that belongs to an Archival series (such as executive committee papers) will be managed as Archival from the point of creation. Refer to University Archives - Archival Series.

e) The University and individual areas will comply with the Privacy Procedures with regards to the creation, collection and capture of personal information. This may include completing a Privacy Impact Assessment (PIA). Refer to the PIA checklist to determine when a PIA is required. In the case of researchers collecting and/or using personal and sensitive personal information, the need to complete a PIA is identified as part of the Research Data Management Plan (RDMP) process.

3.3 CLASSIFY

a) Data and information will be classified as per the Information Security Classifications (refer to the descriptions and examples in Appendix A) unless it sits outside of the Classifications as outlined in the Information Management Policy. Refer to the Information Security Classification Toolkit for further guidance on how to determine and apply the Classifications.

b) Where applicable and feasible, data and information will be labelled with the relevant classification at the point of creation. See Information Security Classification Toolkit.

c) In the case of data and information held in Business Information Systems and other DTS supported systems where the data and information are an aggregation, and it is not feasible to classify each element separately, then a classification is to be applied at the system or aggregation level.

d) The Information Security Classification of data and information will be reviewed if the sensitivity and/or value of data and information changes during the lifecycle. Where the current classification is no longer appropriate then individuals and areas will ensure the data and information will be reclassified.

e) Where appropriate files and folders are to be given titles that reflect the content and context of the data and information they contain (Refer to the Document Naming Guidelines). Where feasible, systems will store data about the information it holds such as descriptive or technical metadata that can be used to make decisions about how to handle the data and information it stores. Where data and information are of historical or Archival value additional metadata will need to be captured as determined by the University Archivist – see Metadata Guide.

3.4 STORE

a) Wherever possible, individuals and areas are to ensure that data and Information in digital form will be stored in Curtin supported systems, unless there is a contractual or technical requirement to use alternative storage. Data in hard copy form will be stored in locations appropriate to its Information Security Classification. Refer to the *Privacy Procedures* and Where to Store Information.

b) When non-Curtin supported systems are used, the risks of using alternative storage are to be considered and mitigated wherever possible.

3.5 USE, SHARING AND DISCLOSURE

a) Data and information will be handled according to its sensitivity as determined by its Information Security Classification (see Information Security Classification Toolkit).

b) The University, through the FOI Coordinator, is to comply with requirements to release information under the *Freedom of Information Act 1992* (WA), with the exception of Global campuses who must comply with any local requirements in their country with regards to freedom of information.

c) The University community will comply with the Privacy Procedures and/or Disclosure of Personal Information Procedures with regards to using, sharing or disclosing any personal or sensitive information to any individual, entity or other third party under contract, collaboration, licence, project or agreement or other relevant situation.

3.6 RE-USE and MAINTAIN

a) Any real or suspected loss, theft or unauthorised access of personal data or information will be reported in accordance with the *Information Breach Policy*. Global campuses will abide by any local requirements in their country for management and reporting of data breaches.

b) Processes will be put in place, and followed, so that data and information, along with its associated metadata, remains discoverable, accessible and useable by those authorised to access it, over its lifecycle regardless of the repository or system within which it is stored.

c) The data and information managed by Individual Areas will be included in their business continuity and disaster recovery planning.

d) Data and information will be retained and maintained for the appropriate minimum time as determined by the relevant Retention and Disposal Authority regardless of when it was last used and regardless of format.

3.7 ARCHIVE and PRESERVE

a) Hard copy data and information of historical or Archival value will be identified, retained, preserved and, where feasible, transferred to the custody of CIMA as soon as practicable after the Area is no longer actively using it.

b) Relevant Areas will ensure that digital data and information of historical or Archival value will be identified, retained and preserved by undertaking digital preservation actions such as providing appropriate preservation metadata and moving digital content to newer file formats or repositories.

3.8 DELETE or DESTROY

a) Individuals and Areas will take reasonable steps to avoid retaining data and information beyond its minimum retention period as set out in the Retention and Disposal Authorities, unless there is a University, regulatory or legal reason to retain it and the risks of over retaining the information have been assessed. (Refer to the Information Handling Guideline.)

b) With the exception of the items covered in 3.8(c), approval will be sought from CIMA prior to destruction or deletion of data and information (see Disposal of Information).

c) Certain types of low value, low risk data and information that do not require CIMA approval before deletion or destruction, are to be deleted or destroyed as soon as they are no longer needed, such as:
   - low value routine transitory messages giving minor instructions of a routine instructional nature that are used to further some activity,
   - exact duplicate files
   - Personal Information collected for proof of an individual's identity
   - other types of information as set out in Disposal of Information.

d) Hard copy data and information that has been digitised will only be destroyed if it meets certain conditions (see Scanning Documents). If conditions are not met, it cannot be destroyed.

3.9 In addition to the responsibilities above the following responsibilities apply.

Global campus staff will:

a) Abide by Freedom of Information requirements that relate to their jurisdiction.

b) Abide by privacy requirements that relate to their jurisdiction.

c) In lieu of clause 3.5 (b), abide by any requirements in their country for management and reporting of data breaches.

Managers (e.g., Heads of School/ Area/ Organisational Area) will:

a) Foster and support a culture that promotes good information management practices.

b) Ensure that all individuals in their area are informed of, the University's Information Management policies and procedures.

Director, Data and Information Governance will:

a) Ensure that data and information governance strategies and policies support the Procedure.

b) Develop and maintain a data and information governance framework.

c) Develop risk management capability across the University in relation to data and privacy.

d) Develop and monitor the University's approach to the management of all data and information.

Associate Director, Curtin Information Management and Archives will:

a) Ensure the development and implementation of policies and frameworks within which the Procedures are to operate.

b) Ensure the development and implementation of best practice guides, tools, education and training on information management to support the University Community in meeting these Procedures.

c) Provide advice to the University Community on matters related to the management of information.

d) Monitor compliance with information management policies and procedures.

e) Advise senior management of risks associated with non-compliance or poor data and information management

University Archivist will:

a) Determine what data and information, whether digital or physical, is suitable for the University Archives.

b) Mediate donations and transfers of material to and from the University.

c) Manage changes to Information Security Classifications of Restricted Access Archives to enable public access after certain periods in accordance with the Western Australian University Sector Disposal Authority (WAUSDA) (Introduction Item 2.3 Restricted Access Archives).

d) Enable appropriate access to the University Archives.

e) Undertake active preservation of both physical and digital Archives.

Privacy Officer will:

a) Prepare, review, and provide guidance and training on the University's Privacy Policy and Privacy Procedures

b) Prepare, review, and provide guidance and training on the University's Information Breach Policy and Information Breach Procedures

c) Oversee processes for undertaking Privacy Impact Assessments (PIA) and conduct PIAs in consultation with project leads and business units

d) Manage and coordinate privacy complaints and reports made under the Information Breach Procedures

Business Information System Owners (e.g. Manager, Student Systems) will:

e) Ensure the system processes and controls are in place such that individuals are provided with the required level of access to data and information in order to effectively carry out their activities.

f) Ensure effective controls are in place to support appropriate information handling in line with the Information Handling Guideline.

a) Ensure the system is captured in Curtin's Information Asset Register.

b) Ensure the systems hold sufficient metadata to describe the content, structure and context of the data and information held in the system throughout the lifecycle of the Information. (See Metadata Guide)

c) Contact CIMA prior to decommissioning Business Information Systems.

d) Work with CIMA with regards to the preservation of data and information where it is deemed that the Business Information System contains Archival data and information.

e) Complete a Privacy Impact Assessment prior to commencement of any project, system roll out, collaboration, licence or agreement which will use, disclose or share personal or sensitive information.

4. SCOPE OF PROCEDURES

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)

Accessibility
Accessibility refers to the design and provision of products, services, environments, and information in a way that ensures people with disabilities can access and use them effectively, independently, and with dignity. It is a vital aspect of promoting diversity, equity, and inclusion in society. In the context of this Procedure, accessibility can also refer to the availability of information in the sense that authorised users can access information or systems whenever they need it, without interruption or delay.

Archives
Data and information, in any format, that is preserved *permanently* because of its enduring significance and value. Archives provide evidence of university functions, programs, issues and associated decisions that are sufficiently critical, important or memorable that they warrant permanent retention. They may relate to social, economic, political, environmental, national security, historical, cultural, scientific and legal impact.

Business Information System
Systems that capture and manage information about an organisation's functions and activities to support the goals and purpose of the organisation, such as:

- Financial Management
- Human Resource Management
- Student Management
- Customer Relationship Management

Business Information System Owner
The individual authorised by the University with responsibility for the overall procurement, development, integration, modification, operation, maintenance and retirement of an information system. Examples include the business owner of Student One or Finance One.

Data
Facts, statistics, or information that are collected for analysis, reference, decision-making and to gain knowledge and insights. It serves 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.

Metadata
Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. Examples of metadata include author, date created, title, date last modified and by whom, etc.

Preservation
Preservation encompasses the activities which prolong the usable life of Archival material. Preservation activities are designed to minimize the physical and chemical deterioration of material and to prevent the loss of informational content and metadata. Hard copy archives activities include providing a stable environment for material of all media types. Activities for digital material include active ongoing management of digital data, such as migrating data to newer formats, creating multiple copies, backup systems and fixity checking.

6. SCHEDULES

N/A

7. RELATED DOCUMENTS/LINKS/FORMS

Accessible Information Procedures
Archives Collecting Statement
Australian Privacy Principles
Curtin Information Management and Archives website (Staff only)
Disclosure of Personal Information Procedures
Disposal of Information guide
Diversity, Inclusion and Belonging Policy
Document Naming Guidelines
Higher Education Standards Framework (HESF): Standards 2.1.2 & 7.3.3
Freedom of Information Act 1992 (WA)
Information and Communication Technology Appropriate Use Procedures
Information Breach Policy
Information Breach Procedures
Information Handling Guide
Cyber Security & Information & Communications Technology (ICT) Appropriate Use Policy
Information Security Classifications Summary Table
Information Security Classification Toolkit
Intellectual Property Policy
Metadata Guide
Privacy Impact Assessment (PIA Checklist)
Privacy Policy
Privacy Procedures
Research Data Management Plan portal
Retention and Disposal Authorities (staff use)
Retention and Disposal Authorities (student use)
Scanning documents guide
University Archives – Archival Series
Western Australian University Sector Disposal Authority (WAUSDA)
Where to store information best practice guide

Policy Compliance Officer	Krista Bell, Director, Data and Information Governance
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2029

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

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
H001/P6.1	Approved	30/09/2003	Planning and Quality Committee	PMC 95/03	Document No 63/03
H001/P6.1 A	Amended	25/10/2006	Council	C 150/06 (iii)	Document No 01108/06
H001/P1.6 B	Amended	09/05/2007	Council	C 58/07	Document No 00390/07
	Administratively Updated	20/03/2008	Director, Legal and Compliance Services		Reformatted and Amended to Reflect Organisational Chart
	Administratively Updated	16/10/2012	Director, Legal and Compliance Services		Policy Contact Updated
	Administratively Updated	06/10/2015	Director, Legal and Compliance Services	EC 76/15	Executive Manager Title Changes
	Amended	22/01/2016	Chief Operating Officer	EM1602	Unconditional
	Approved	25/03/2021	Chief Operating Officer	EM2144	Name changed from Records and Information Management Procedures
	Approved	16/02/2026	Chief Operating Officer	EM2601	Unconditional

APPENDIX A

INFORMATION SECURITY CLASSIFICATIONS[#]

CLASSIFICATIONS	DESCRIPTION	EXAMPLES

PUBLIC	Official University data and information that has been authorised for public access and circulation or deemed public by legislation or routine disclosure.
	
	No access restrictions or special handling are required.
		Examples include:
		• University public facing web pages
		• Published course information (Curtin Handbook)
		• Information for prospective students
		• Released media statements
		• Academic calendar
		• University Annual Reports and published Strategic Plan
		• University Policies and Procedures published on the Find a Policy webpage
		• Campus maps
		• Brochures and other promotional materials or information
		• Researcher summary profiles published for the purposes of supervision or expertise
		• Research related information (including data) that has been published openly which may be downgraded to this classification such as:
		  • Appropriately de-identified aggregated research data
		  • Non-sensitive data from sensors and cameras with containing no personal information
		  • Non-sensitive data from instruments and imaging systems

INTERNAL	This classification is appropriate for much of the information created, used or handled by the University. This includes routine business operations and services where the information is not for general public release. It is for internal Curtin use (and limited authorised external audiences).
	
	Some access restrictions and special handling are required.
		This is the default classification for all University information except:
		• research data
		• information related to research projects
		• personal information
		
		Examples include:
		• Intranet sites and other internal facing web pages
		• Operational plans for Schools and Areas
		• Teaching materials
		• Operational meeting agendas and minutes which do not contain or relate to sensitive information
		• Employee directories (where information is not publicly available)
		• Research-related information which does not contain sensitive information which may be downgraded to this classification. Examples might include:
		  • Appropriately de-identified aggregated research data
		  • Non-sensitive data from sensors and cameras containing no personal information
		  • Non-sensitive data from instruments and imaging systems
		  • Drafts of research publications

CLASSIFICATIONS	DESCRIPTION	EXAMPLES

SENSITIVE	This classification is for information that commonly includes 'sensitive' or confidential material created, used or handled by the University. Such information is for limited audiences within Curtin (and limited authorised external audiences – e.g., research collaborators).
	
	Several sub-categories can be applied to indicate the nature of the data and information and that access restrictions and special handling is required:
	• **SENSITIVE** – Legal
	• **SENSITIVE** – Personal
		This is the default classification for research data and information related to research projects, as well as Personal Information (PI) as defined under the Privacy and Responsible Information Sharing Act 2024 (including Sensitive Personal Information).
		
		Examples of **SENSITIVE** information include:
		• Information related to research projects, including ethics approvals, management of the project, and foreign risk reviews.
		• All research data created by Curtin staff or Higher Degree by Research (HDR) students held by, or in, University systems (unless the classification is changed to a higher or lower classification).
		• Secretariat-supported committee agendas and minutes and non-Secretariat-supported committees or groups containing or relating to sensitive information of individuals or sensitive research (e.g., Promotions assessment panels).
		• Exam papers – both master sets and student completed exam scripts.
		• Exam results and grades.
		• Password and cryptographic key information.
		• Organisational financial data.
		• Intellectual property containing trade secrets or other commercially sensitive Intellectual Property.
		• Information provided to the University as commercial-in-confidence or under a Non-Disclosure Agreement.
		
		Examples of **SENSITIVE – Legal** information would be that which is subject to legal professional privilege
		
		Examples of **SENSITIVE** – Personal information include:
		• Information in any form that reasonably identifies an individual that is collected and held by the University for teaching, research or administrative purposes (including Sensitive Personal Information) such as:
		  • Name, contact information (including addresses), date of birth, gender and unique identifiers.
		  • Images, audio or video recordings (e.g., from volunteers or as part of a research project or collected during University recruitment events).
		  • Information about individuals related to employment or association with Curtin (e.g., Tax File Numbers, passport details, bank account details, Police Clearances).

CLASSIFICATIONS	DESCRIPTION	EXAMPLES
		• Biometric data of individuals (e.g., fingerprints or other data used for facial, voice and iris or retina recognition) • Student information (e.g., Student ID, grades, progression information, credit card numbers, passport details). • Student discipline matters • Alumni and donor information. • Research data involving personal information. • Health, medical and counselling patient files.
RESTRICTED	This classification is for information that commonly includes highly 'sensitive' or confidential material created, used or handled by the University. Such information is for strictly limited audiences within Curtin (and strictly limited authorised external audiences – e.g., research collaborators). Several sub-categories can be applied to indicate the nature of the data and information. Access restrictions and special handling is also required: • **RESTRICTED** – Personal	Examples of **RESTRICTED** information include: • Research data that, if released, could cause serious harm to an individual or organisation. Examples of **RESTRICTED** – Personal • Personal information that, if released, could cause serious harm to an individual such as address/contact details of a vulnerable person.

Notes
[#] Refer to the University Impact table for information on the level of impact and harm that would reasonably be expected if the information in each classifications was compromised.

The above classifications are to be applied except where Curtin is contractually obliged to apply other classifications (e.g. Protective Security Policy Framework) or existing classifications apply (e.g. data from third parties).