Curtin University

Information Management Procedures

1. STRATEGIC PLAN THEME AND COMPLIANCE OBLIGATION SUPPORTED

Information Management Policy

Strategic Plan Theme: Sustainable Future

2. PROCEDURAL DETAILS

This document outlines the procedures for the creation and management of information that documents the University's business activities and provides evidence of University decisions, transactions and actions.

2.1 Information requires effective management throughout the information lifecycle to ensure that it is appropriately secured to safeguard its authenticity, integrity, reliability, useability and is used for the purposes intended throughout its lifecycle.

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

2.3 Information created or received during the course of Curtin business is vested in the University and remains under University control unless:

- There is a written agreement in place stating that the Information is owned by other parties, or;
- The Information constitutes Intellectual Property that is vested in an individual as per the University's Intellectual Property Policy.

2.4 Responsibilities

Position	**Responsibilities**
2.4.1 All individuals regardless of location	**Creation and storage of Information** a) Wherever possible, identifying potential future Archives at the point of creation and contacting the University Archivist for assessment close to the point of creation. **b)** Storing Information in approved Curtin systems, unless when contractually required to use alternative storage. Refer to Where to Store Information. **Classification and metadata** c) Classifying Information as per the Information Security Classification Policy and labelling it with the relevant category at the point of creation then updating it at any point that the category changes. (See Information Security Classification Matrix). d) Naming Information appropriately by providing basic metadata as per the Document Naming Guidelines. **Protection, access and use of information** e) Complying with any restrictions or obligations with regards to the sharing, printing, copying and use of Information as required by: ○ the Information Security & Information & Communication (ICT) Appropriate Use Policy ○ the Information and Communication Technology Appropriate Use Procedures ○ the Disclosure of Personal Information Procedures ○ the University's Privacy Statement ○ the Information Security Classification category assigned to the information ○ any contractual requirements related to the Information

	○ any legislative requirements to release information (including to regulators) f) Complying 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. g) Consulting with the Information Disclosure Compliance Officer (IDCO) prior to commencing a project, pilot program or integration of data that involves Personal Information held by the University, to determine if a Privacy Impact Assessment (PIA) is required. Individuals undertaking research projects that may involve Personal Information are required to complete a Data Management Plan. h) Reporting any real or suspected loss, theft, unauthorised access or unauthorised disposal of Information to Curtin Information Management and Archives and the IT Security and Assurance Team. i) If the Information in h) involves Personal Information then, with the exception of Global campuses, individuals must: ○ Contact the Information Disclosure Compliance Officer (IDCO) and ○ Report the incident via the ISU Complaints Portal Global campuses will abide by any local requirements in their country for management and reporting of data breaches. **Retention and Disposal of Information** j) Deleting or destroying certain types of Information, such as low value transactional Information, as part of normal administrative practice, where formal destruction approval is not required (see Disposal of Information). k) Destroying hard copy Information that has been digitised only if it meets certain conditions (see Scanning Documents). If conditions are not met, it cannot be destroyed. l) Ensuring that all other Information must only be deleted or destroyed in accordance with the set retention periods outlined in the University's Disposal Authorities and with approval from Curtin Information Management and Archives. m) Ensuring that Information of historical or archival value is retained and transferred to the custody of the University Archivist.
2.4.2 Global campus staff	In addition to 2.4.1: a) Abiding by freedom of Information requirements that relate to their jurisdiction. b) Abiding by privacy requirements that relate to their jurisdiction. c) In lieu of clause i) above, abiding by any requirements in their country for management and reporting of data breaches.
2.4.3 Managers (e.g., Heads of School/ Area/ Organisational Area)	In addition to 2.4.1: a) Approving the use of alternative storage mechanisms for Curtin Information (other than Curtin's approved systems) based on the review of a risk assessment. b) Fostering and supporting a culture that promotes good information management practices. c) Ensuring that all individuals in their area are informed, and abide by, the University's Information Management policies and procedures.
2.4.4 Associate Director, Curtin Information	In addition to 2.4.1: a) Ensuring the development and implementation of policies and frameworks within which the Procedures are to operate.

Management and Archives	b) Ensuring 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) Providing advice to the University Community on matters related to the management of Information. d) Monitoring compliance with information management policies and procedures. e) Advising senior management of risks associated with non-compliance or poor information management
2.4.5 University Archivist	In addition to 2.4.1: a) Determining which materials are suitable for the University Archives. b) Mediating donations and transfers of material to the University.
2.4.6 Business Information System Owners (e.g. Manager, Student Systems)	In addition to 2.4.1: a) Ensuring the systems hold sufficient metadata to describe the content, structure and context of the Information held in the system throughout the lifecycle of the Information. (See Metadata Guide)

3. RESPONSIBILITIES

Responsibilities are those as set out in Section 2.

4. SCOPE OF PROCEDURES

This procedure applies to all staff, adjuncts, associates and students who manage University Information in any location or campus, whether in or outside of Australia.

5. DEFINITIONS

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

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.

Information
Any records, data, documents and files (including but not limited to data contained in databases or business systems, emails, social media posts, webpages, audio visual files, research data, plans, spreadsheets) in any form created, received and maintained in the course of undertaking Curtin business. Non-work related information created, received or saved by individuals into Curtin systems is also included in this definition.

Metadata
Data describing context, content and structure of records which enables the creation, use and management of these records through time within and across domains. Examples of metadata include author, date created, title etc.

Personal Information
Information (including information forming part of a database), and whether recorded in a material form or not, about an individual whose identify is apparent, or can reasonably be ascertained, from the information.

6. SCHEDULES

N/A

7. RELATED DOCUMENTS/LINKS/FORMS

Australian Privacy Principles
Curtin Information Management and Archives website
Disclosure of Personal Information Procedures
Disposal Authorities
Disposal of Information guide
Document Naming Guidelines
Freedom of Information Act 1992 (WA)
Information and Communication Technology Appropriate Use Procedures
Information Management Policy
Information Security and Information and Communications Technology (ICT) Appropriate Use Policy
Information Security Classification Matrix
Information Security Classification Policy
Intellectual Property Policy
ISU Complaints Portal
Metadata Guide
Research Data Management Plan portal
Scanning documents guide
Where to store information best practice guide

Policy Compliance Officer	Sue Aldenton, Associate Director, Curtin Information Management and Archives
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2021

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board/ Executive Manager	Approval / Resolution Number	Key Changes and Notes
H001/P6.1	Approved	30/09/2003	Planning and Quality	PMC 95/03	Document No 63/03
H001/P6.1A	Amended	25/10/2006	Council	C 150/06 (iii)	Document No 01108/06
H001/P1.6B	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