

Information Classification Procedure

Purpose and Scope

Provides the procedure and responsibilities for information classification in all formats across the University.

This procedure applies to:

- All staff, students, consultants, authorised contractors, and volunteers, engaged in Murdoch University activities.
- All information in all its forms, created, collected, processed, or stored on Murdoch University equipment or cloud services.

Overarching Policy

[Information Classification Policy](#)

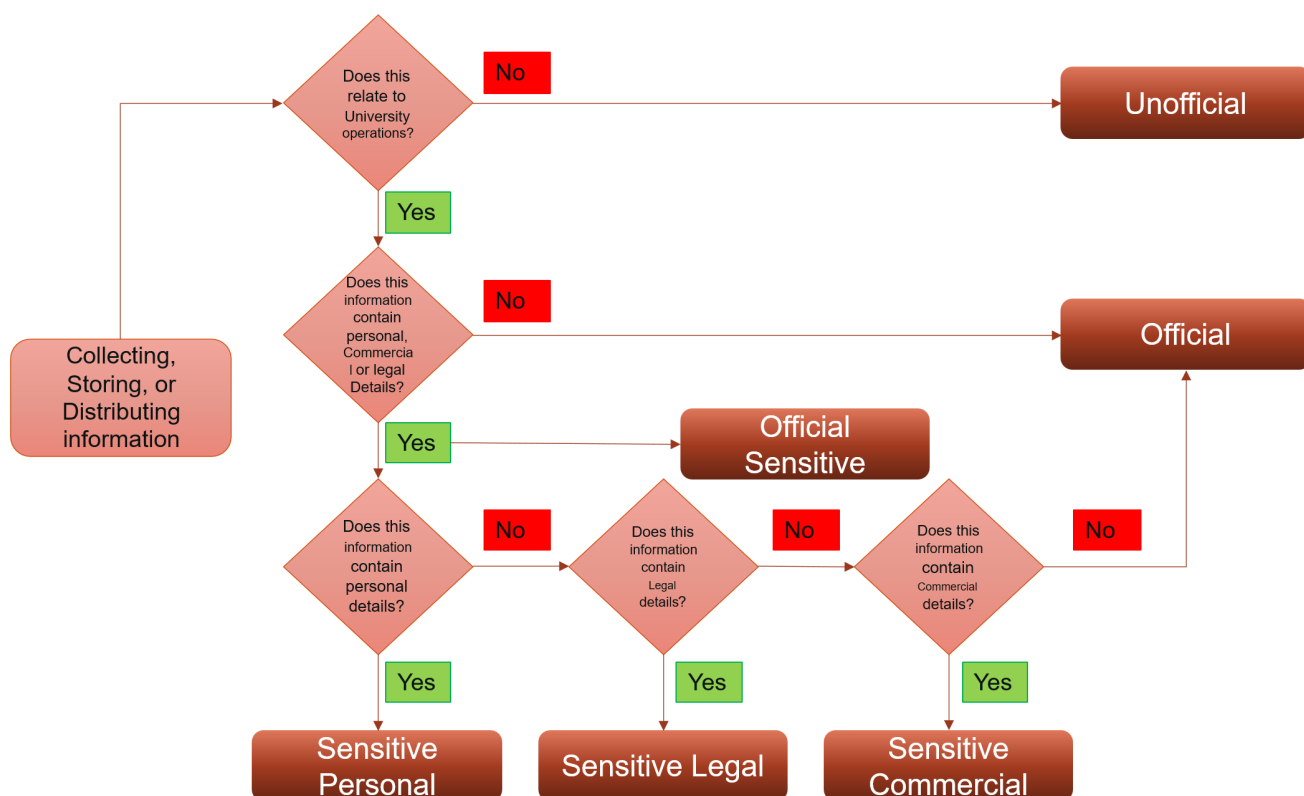
Procedure

1. Information must be classified in accordance with this Procedure and managed in line with the Handling Guidelines.
2. Before information is collected, stored or distributed, individuals must ensure that it is:
 - a) Classified according to the classification labels outlined in Table 1.
 - b) Limited to only that information which is necessary for the purpose.
 - c) Reported immediately to their line manager where sensitive information is shared with an unauthorised party, exposed in an uncontrolled environment, or accidentally received.
 - d) Referred to their line manager where a change to the information classification is required.
3. Documents will have the classification label “Official” by default. Classification labels are currently enabled in Microsoft Word, Excel, PowerPoint and Outlook. Default classification label implementation across other systems is in progress.

Table 1: Classification labels with description and examples

Label	Description	Examples
Unofficial	Information that is not related to official work.	• Personal holiday plan • Invitations for coffee catchups
Official	Information related to routine business operations and services. Compromise of the information would be expected to cause minor harm to University's staff and stakeholders.	• Routing business operations emails • Briefing notes • Policies and Procedures
Official Sensitive	Information related to routine business operations and services with sensitive details. Compromise of the information would be expected to cause Moderate, Major, and Extreme harm to University's staff and stakeholders	• Student and staff personal information. • Performance Management Files • Exam Papers • Exam Results • Supplier Invoices
Sensitive Personal	Information with personally identifiable and sensitive details.	• Employee Health Files • Student Discipline Files • Employee files • Identifiable research data relating to individuals
Sensitive Commercial	Information with commercial sensitive details	• Commercial Agreements • Research Data • New Designs
Sensitive Legal	Information with legal details	• Legal advice • Legal Communications

Decision Flowchart



Handling Guidelines

Handling Official Information

Labelling	Document must include the label 'Official' on the cover page or where no cover page exists, on the first page.
Cloud (One Drive/ SharePoint) & Network Storage	Information may be stored in Murdoch University- authorised SharePoint sites, approved cloud storage services, and network drives. Information must not be stored in personal or unapproved online storage.
Portable Storage (USB Drives, Portable Hard Drive)	Use of portable storage is not recommended. Where portable storage is used, appropriate care must be taken to prevent data loss. Portable storage is not backed up by the University and data may not be recoverable.

Hard Copy Storage	Hard copy information must be store in a closed container and managed in accordance with the requirements of the University Sector Disposal Authority or the General Retention and Disposal Authority for State Government .
Emails	Emails must have the 'Official' label applied. Official information may be included as email attachments.
Generative AI agents	Use of Murdoch University–approved AI agents is recommended. University information must not be uploaded, shared, or processed using unapproved or public AI tools.
Access – University Employees	Access to official information is permitted to authorised Murdoch University account holders (i.e. with a murdoch.edu.au account). Access is limited to authorised University employees within the relevant working group.
Access – External Parties	A formal confidentiality agreement must be in place prior to accessing information through University systems or at the onboarding process. Information may be sent externally during normal business operations.

Handling Official Sensitive, Personal Sensitive, Commercial Sensitive and Legal Sensitive Information

Labelling	Document must, at a minimum, include the label “Personal Sensitive, Commercial Sensitive or Commercial Sensitive” on the cover page and in the header or footer of every page.
Cloud (One Drive/ SharePoint) & Network Storage	Information may be stored in Murdoch University–authorised SharePoint sites, approved cloud storage services, and network drives. Information may not be stored in personal or unapproved online storage.
Portable Storage (USB Drives, Portable Hard Drive)	Sensitive information must not be stored on portable storage devices.

Hard Copy Storage	Hard copy information must be stored in a secure, closed container, such as a locked cabinet or access-controlled office, and managed in accordance with the requirements of the University Sector Disposal Authority or the General Retention and Disposal Authority for State Government .
Emails	Emails must have the appropriate sensitivity label applied. Emails containing sensitive information must not be automatically forwarded to non-Murdoch-controlled email addresses. Manual forwarding to external recipients is only permitted where authorised and in accordance with University policy.
Generative AI agents	Only Murdoch University–approved AI agents may be used.
Access – University Employees	Access must be approved by the Information Custodian prior to being granted.
Access – External Parties	A formal confidentiality agreement must be in place prior to accessing or receiving information

Roles and Responsibilities

Roles	Responsibilities
Information Owners Senior Leadership Team	• Ensure that information is evaluated and classified in accordance with the information classification system outlined in this procedure. • Oversee the completion of responsibilities to Information Stewards, where appropriate.
Information Stewards Senior Leadership Member	• Implement data management policies for their functional areas. • Liaise with relevant staff to determine information classifications. • Can change the applied label when required. • Ensure appropriate safeguards are implemented to protect data from unauthorised access and loss. • Ensure Murdoch University Information Asset Register is maintained.

	• Maintain, share, and improve information.
Information Custodians Team Manager/Leader	• Provide a secure physical and system control framework to protect information. • Approves access to relevant 'Official Sensitive' information. • Can change the applied label when required. • Maintain information lifecycle management, backup and recovery processes, and monitor access privileges. • Handle information in accordance with its classification and authorised purpose. • Protect the confidentiality, integrity, and availability of information.
Information Creators and Users	• Comply with this Procedure and relevant University policies pertaining to the creation, use, collection, storage and sharing of information. • Apply the correct classification at the point of creation. • Handle information in accordance with its classification and authorised purpose. • Protect the confidentiality, integrity, and availability of information. • Report suspected or actual information security incidents.

Governance

Approval Authority	Senior Leadership Team
Owner	Vice Chancellor
Legislation mandating compliance	<u>General Retention and Disposal Authority for State Government Information DA 2023-004</u> <u>Western Australia University Sector Disposal Authority</u> <u>Privacy and Responsible Information Sharing Act 2024</u> <u>State Records Act 2000</u>
Category	Primarily a function of management

Related University Legislation and Policy Documents	<i>Information Management Policy</i>
Date effective	29/06/2026
Review date	12/08/2027

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Approved by SLT	29/06/2026	
Administrative Amendment	26/03/2025	
Administrative Amendment	04/09/2024	
Approved	12/08/2024	

Please refer to the electronic copy in the Policy and Procedure Manager to ensure you are referring to the latest version.