

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 university equipment or cloud services.

Overarching Policy

[Information Classification Policy](#)

Procedure

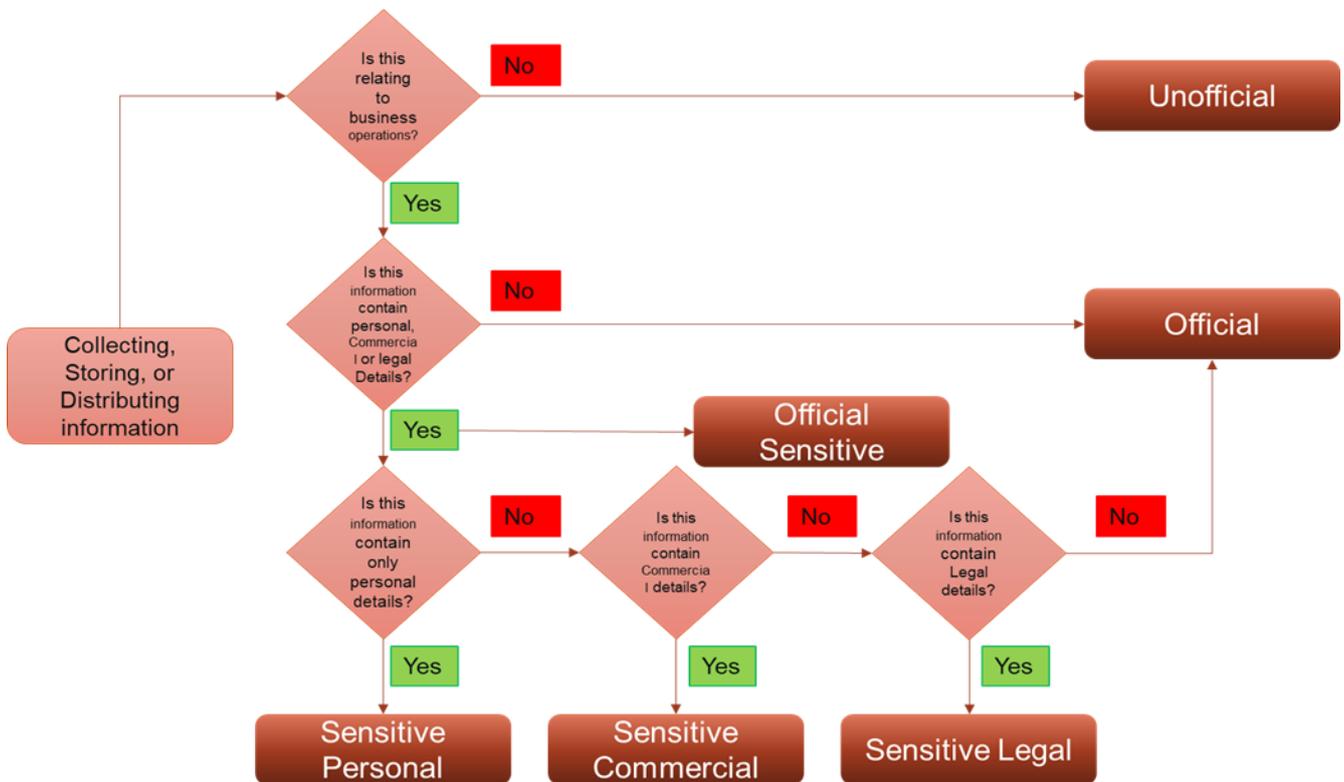
1. Information must be classified following this procedure and handling guidelines.
2. Before collecting, storing, or distributing information, all staff, students, consultants, authorised contractors, and volunteers, engaged in Murdoch University activities must ensure they:
 - 2.1. Classify the information where possible.
 - 2.2. Minimise the information to only which is required where possible.
 - 2.3. Notify their direct report immediately, if highly sensitive information is shared with an unauthorised party, exposed in an uncontrolled environment, or accidentally received.
 - 2.4. Consult their Business Unit manager if required to change the classification.
3. Personal Sensitive Information: - Information with personally identifiable and sensitive details. This can include information about an individual's academic, work or business activities. Examples include an individual's: name, gender, date of birth, age, signature, address, contact details (phone, mobile, email addresses), staff and student ID, financial/banking/credit information,

health/medical information, Medicare Card details, mother/father’s name, name of school, social security number, driver's license number, passport number, patient ID number, and taxpayer ID number.

4. University information should be categorised into one of the following classifications. Information Stewards and Custodians can change the applied label when required.
5. Documents will have the label “Official” by default. Labels are enabled in Microsoft Office, Excel, Power point and Outlook currently and applying to other systems are in progress.

Label	Description	Examples
Unofficial	Information that is not related to official work.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Student and staff personal information. • Performance Management Files • Exam Papers • Exam Results • Supplier Invoices
Sensitive Personal	Information with personally identifiable and sensitive details.	<ul style="list-style-type: none"> • Employee Health Files • Student Discipline Files • Employee files • Identifiable research data relating to individuals
Sensitive Commercial	Information with commercial sensitive details	<ul style="list-style-type: none"> • Commercial Agreements • Research Data • New Designs
Sensitive Legal	Information with legal details	<ul style="list-style-type: none"> • Legal advice • Legal Communications

6. Decision Path



7. Handling Guidelines

7.1. Handling Official Information

Labelling	Document should include 'Official' on the cover page or first page.
Cloud (One Drive/ SharePoint) & Network Storage	Can be saved in Cloud/Network Storage access limit to all users with Murdoch access account.
Portable Storage	Saving on Portable Storage not recommended. Appropriate care must be taken to prevent data loss when saving content.
Hard Copy Storage	Store within a closed container with appropriate retention from University Sector Disposal Authority or General Retention and Disposal Authority for State Government.
Emails	Select 'Official' Label. Can be included as email attachments.
Access – University Employees	No restrictions for Anyone who holds a Murdoch.edu.au account / Relevant access within the working group
Access – External Parties	Sign formal confidentiality agreement prior to access or at the onboarding process when accessing through the

University's systems. Information may be sent externally during normal University business.

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

Labelling	Document should include least 'Official Sensitive' on the cover page and header or footer of each page.
Cloud (One Drive/ SharePoint) & Network Storage	Can be saved in Cloud/Network storage with restricted access to authorised employees or group.
Portable Storage	Do not save on Portable Storage.
Hard Copy Storage	Store within a secure, closed container, locked cabinet or access-controlled office. Apply appropriate retention from University Sector Disposal Authority or General Retention and Disposal Authority for State Government.
Emails	Select appropriate label on the email.
Access – University Employees	Obtain Information Custodian's approval prior to granting access to information.
Access – External Parties	Sign formal confidentiality agreement prior to accessing or receiving information.

Roles and Responsibilities

Role	Responsibility
Information Owners Senior Leadership Team with authority and accountability for Information within their functional areas.	<ul style="list-style-type: none"> Ensuring that information is evaluated and classified in accord with the information classification system outlined in this policy. Overseeing the completion of responsibilities to Information Stewards, where appropriate.
Information Stewards (Senior Leadership Member from the	<ul style="list-style-type: none"> Implementing data management policies for their functional areas.

respective functional area)	<ul style="list-style-type: none"> • Liaising with relevant staff to determine security classifications. • Ensuring appropriate safeguards are implemented to protect data from unauthorised access and loss. • Ensuring Murdoch University Information Asset Register maintained. • Maintaining, Sharing, and Improving information.
Information Custodians (Manager/Leader from the respective Team)	<ul style="list-style-type: none"> • Maintaining physical custody of institutional Information. • Providing a secure physical and system control framework to protect data. • Maintaining information lifecycle management, backup/ recovery processes, and monitoring access privileges. • using best practice to maintain the confidentiality, integrity and availability of information.
Information Creators and Users	<ul style="list-style-type: none"> • Complying with relevant University policies pertaining to the creation, use, collection, storage and sharing of information. • biding by requirements to protect the confidentiality, privacy and integrity of data and handle information and data commensurate with its information classification.

Governance

Approval Authority	Senior Leadership Team
Owner	Vice Chancellor
Legislation mandating compliance	
Category	Primarily a function of management
Related University Legislation and Policy Documents	<u>Information Management Policy</u>
Date effective	26/03/2025

Review date

12/08/2027

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
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.