Information Classification and Handling Procedures

Table of Contents

1. Governing Policy

Digital Security Policy

2. Purpose

To outline the process for classification and handling of the University’s information assets.

3. Definitions

Highly confidential information	Information containing research, educational, enterprise or personally identifiable data that if released could result in major or severe financial, reputation or legal impact to the University or an affiliated organisation or individual. Examples include medical records and work cover forms.
Information classification	A systematic method for assessing and documenting the protection requirements of data or a collection of data (information) to ensure the University can meet security, confidentiality, integrity, availability, and retention requirements.
Internal use only information	Information not intended for public release, but unintended disclosure causes only minor or insignificant impact to the University or an affiliated organisation or individual. Examples include day-to-day correspondence, project and administrative documentation.
Personally Identifiable information	Personal information (PI) is defined in the University’s Privacy Policy. PI becomes Personally Identifiable Information (PII) when the information can distinguish and/or trace an individual identity. This PII is either used in isolation or with other personal information such as email, home address, and staff/student ID. For example, using a person’s full name, address, and student ID to contact them.
Public information	Information that is intended for the public domain or that has been approved for release to the public. Examples include student course information,

	research data made public, marketing material, website content and press releases.
Restricted information	Information containing research, educational, enterprise and/or personally identifiable data that if released could result in minor or moderate financial, reputation or legal impact to the University or an affiliated organisation or individual. Examples include student records including academic results or analytics data, staff records, unpublished research reports or data, audit reports and Council papers.
Research data	Includes the primary materials and analysed data, records, results, files or other evidence that allows for the justification and verification of research outcomes, irrespective of the content or format of that evidence.
Sensitive information	Sensitive information is defined in the Privacy Policy. Sensitive information is not disclosed to the public. When linked to an identifier, i.e., name, email, staff/student ID, it becomes sensitive personally identifiable information (SPII). SPII can identify a single person. If SPII is lost, stolen or distributed without authority, it could cause theft, harm or embarrassment for the individual. SPII can be categorised independently or with other PI, PII and SI components.

4. Procedures

4.1. Determining information classification

a. University staff are responsible for assigning an information classification to any information or document they create, in alignment with these procedures.

b. The assignment of classification is primarily driven by the potential for adverse impact to the University. For example, higher information classifications are to be assigned where more restrictive information handling practices are required.

c. The University has four information classification categories as detailed below.

4.1.1. "Public"

a. The information or service is specifically for public access (e.g., Flinders website or research that has been released).

b. There would be no adverse impact to the University resulting from publication, or such publication is specifically approved.

4.1.2. "Internal Only"

a. The information is not for public access.

b. Accidental or deliberate disclosure, or unauthorised access, to the information would result in minor or insignificant impact to the University.

4.1.3. "Restricted"

a. The information is for limited distribution to specific groups within the University.

b. The information contains research data, educational data, financial data, strategic information, or personal information.

c. Accidental or deliberate disclosure, or unauthorised access, to the information would result in minor or moderate financial, reputational and/or legal impact to the University.

4.1.4. "Highly Confidential"

a. The information is for very limited distribution to specific individuals within the University.

b. The information contains research data, financial data, strategic information, personal information, or sensitive information.

c. Accidental or deliberate disclosure, or unauthorised access, to the information would result in major or severe financial, reputational and/or legal impact to the University.

4.2. Research data

a. All unpublished research data is classified at a minimum as "restricted" and handled and stored accordingly.

b. More sensitive research data is classified as "highly confidential" if it meets the requirements in s.4.1.4 above.

4.3. Educational data and learning analytics

a. All personally identifiable educational and analytics data is classified as "restricted" by default and handled and stored accordingly.

b. Educational and analytics data can be classified as "highly confidential" if it meets the requirements in s.4.1.4 above.

4.4. Digital information asset classification

Division/College owners of digital information assets are responsible for working with Information and Digital Services (IDS) to assign an information classification and criticality to the asset. Based on the agreed classification, IDS may apply additional security measures to manage the associated risk.

4.5. Information reclassification

a. The sensitivity of information can change over time. The owners of information and services are responsible for reclassifying their information as circumstances require. For example, a strategic announcement may begin as a Restricted document, but once approved, may be reclassified as Internal Use Only or Public Information depending on the intended audience.

b. Research data may also be reclassified from Restricted to Public Information once the study has been completed and peer reviewed. Research data may also be reclassified from Restricted to Highly Confidential should the terms of the contract between the sponsoring party and researchers change.

4.6. Handling "public" information

Labelling	No specific requirement to label information at this classification level, unless it is likely to be accessed by third parties.
Cloud/network storage	Network storage does not require access restrictions beyond a limitation to Flinders University community members with a FAN account. Internet-based ("cloud") file storage is allowed for approved providers.
Portable storage	Storage on portable storage devices is allowed without restrictions.
Hard copy storage	No restrictions for printed storage.

Email restrictions	No restrictions for information included as email attachments.
Access by University staff	No access restrictions for university staff.
Access by external parties	No restrictions on legitimate need for access by external parties, although consideration should be given to labelling documents “Internal Use Only” when appropriate.

4.7. Handling “internal use only” information

Labelling	Documents should include label “Internal Use Only” in header or footer of each page.
Cloud/network storage	Network storage does not require access restrictions beyond a limitation to Flinders University community members with a FAN account. Internet-based (“cloud”) file storage is allowed for approved providers.
Portable storage	Encrypt all information on portable storage devices.
Hard copy storage	Printed information should be handled with necessary care to avoid access by external parties including presentation or use within Flinders University buildings or locations and storage in Flinders University buildings or locations.
Email restrictions	No restrictions for information included as email attachments to university staff.
Access by University staff	No access restrictions for university staff.
Access by external parties	External parties must seek approval from the owner of the information based on legitimate need and sensitivity of the documents being requested. There is no automatic right of access.

4.8. Handling “restricted” information

Labelling	Documents should include label “Restricted” in header or footer of each page.
Cloud/network storage	Limit network storage access to authorised **groups** only (for Restricted documents/data). Internet-based (“Cloud”) hosting permitted for Restricted documents, but only for approved storage providers and all data must be encrypted at rest and in transit.
Portable storage	Encrypt all information on portable storage devices.
Hard copy storage	Store within secure closed container, which can include a locked cabinet or locked office within a Flinders University building or location.
Digital transmissions	Physical to digital Digital to digital

	Digital to physical
Email restrictions	Encrypt documents or data before attaching to any email message.
Access by University staff	Obtain approval from the owner of the information prior to granting access to information.
Access by external parties	External parties to sign formal confidentiality agreement prior to information access. There is no automatic right of access.

4.9. Handling "highly confidential" information

Labelling	Documents should include label "Highly Confidential" in header or footer of each page.
Cloud/network storage	Limit network storage access to authorised **individuals** only (for Highly Confidential documents/data). Internet-based ("Cloud") hosting permitted for Highly Confidential documents, but only for approved storage service providers, and data must be encrypted at rest and in transit.
Portable storage	Encrypt all information on portable storage devices.
Hard copy storage	Store within secure closed container, which can include a locked cabinet or locked office. Hard copy document disposal should be performed using a cross-cut shredder and not in the disposal bins.
Digital transmissions	Printing of digital information to produce physical copies is not advised. Obtain approval from the owner of the information prior to printing.
Email restrictions	Encrypt documents or data before attaching to any email message.
Access by University staff	Obtain approval from the owner of the information prior to granting access to information.
Access by external parties	External parties to sign formal confidentiality agreement prior to information access. There is no automatic right to access.

5. Related documents

Privacy Policy

Freedom of Information

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	31 July 2024
Effective Date	31 July 2024
Review Date*	2027
Last amended	
CM file number	CF18/18
* Unless otherwise indicated, this policy or procedures still apply beyond the review date.	

Printed versions of this document are not controlled. Please refer to the Flinders Policy Library for the latest version.