Flinders UNIVERSITY

INSPIRING ACHIEVEMENT

Information Classification and Handling Procedures

Table of Contents

1. Governing Policy

Information Security Policy

2. Purpose

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

3. Definitions

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.
Internal Use Only Information	Information not intended for public release, but unintended disclosure causes only minor or no impact to the University or an affiliated organisation or individual. Examples include day-to-day correspondence, project and administrative documentation.
Restricted Information	Information containing research, educational, enterprise and/or personally identifiable data that if released could result in modest financial, reputation or legal impact to the University or an affiliated organisation or individual. Examples include student records or analytics data, staff records, unpublished research reports or data, audit reports and Council papers.
Highly Confidential Information	Information containing research, educational, enterprise or personally identifiable data that if released could result in critical or serious financial, reputation or legal impact to the University or an affiliated organisation or individual. Examples include medical records and work cover forms.

Digital Information Service	Any technology solution designed to achieve an educational, research or administrative outcome for the University. Includes relevant software, hardware, hosting and licensing components. Includes desktop and enterprise software solutions.
Information Asset	Comprises all forms of data or knowledge, in document or raw data form, that are processed, stored and transferred that have value to the University in electronic or hard copy forms. Digital information services store information assets.

4. Procedures

4.1. Determining information classification

University staff are responsible for assigning an information classification to any document or data they create. The choice of classification is primarily driven by the potential for adverse impact to the University. Higher classifications can result in more restrictive data handling practices.

Determining "Public" Classification	a. The information or service is specifically for public access (e.g. Flinders website, or research that has been released); and b. No adverse impact to University resulting from publication (or such publication is specifically approved).
Determining "Internal Only" Classification	c. The information is not for public access; and d. Accidental or deliberate disclosure or unauthorised access to the information would result in minor or no adverse impact to the University.
Determining "Restricted" Classification	e. The information is for limited distribution to specific groups within the University; and f. Contains research data, educational data, financial data, strategic information or personally identifiable data; and g. Accidental or deliberate disclosure or unauthorised access to the information results in modest financial, reputational and/or legal impact to the University.
Determining "Highly Confidential" Classification	h. The information is for very limited distribution to specific individuals within the University; and i. Contains research data, financial data, strategic information or personally identifiable data; and j. Accidental or deliberate disclosure or unauthorised access to the information results in critical financial, reputational and/or legal impact to the University.

4.2. Research data

a. All unpublished Research data is classified as Restricted by default and handled and stored accordingly.

b. More sensitive Research data can be classified as Highly Confidential by the Information Owner should it meet the requirements 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 by the Information Owner should it meet the requirements above.

4.4. Digital information service classification

a. Business Owners of Digital Information Services are responsible for working with Information and Digital Services (IDS) to assign an information classification and criticality to the service. Based on the agreed classification, IDS may apply additional security measures to manage the associated risk.

4.5. Handling "Public" and "Internal Use Only" information

Labelling	No specific requirement to label information at this classification level, unless likely to be accessed by third parties.
Cloud/Network Storage	• Network storage does not require access restrictions beyond a limitation to users with a Flinders 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 Personnel	No access restrictions for University personnel.
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.

4.6. Handling "Restricted" and "Highly Confidential" information

Labelling	Documents should include label "Restricted" or "Highly Confidential", as appropriate, in header or footer of each page.
Cloud/Network Storage	• Limit network storage access to authorised **groups** only (for Restricted documents/data) or authorised **individuals** only (for Highly Confidential documents/data); • Internet-based ("Cloud") hosting permitted for Restricted documents, but only for approved storage providers; • Highly Confidential information should **not** be stored on Cloud storage services.
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.
Email Restrictions	Encrypt documents or data before attaching to any email message.
Access by University Personnel	Obtain Information Owner approval prior to granting access to information.
Access by External Parties	External parties to sign formal confidentiality agreement prior to information access.

4.7. Information reclassification

a. The sensitivity of information can change over time. Both document and service owners are responsible to reclassify 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 depending on the intended audience. Research data may also be reclassified from Restricted

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	21 December 2017
Effective Date	21 December 2017
Review Date*	December 2020
HPRM file number	CF18/18
* Unless otherwise indicated, this procedure will still apply beyond the review date.	