

## Information Classification and Handling Procedures

### Table of Contents

1. Governing Policy
2. Purpose
3. Definitions
4. Procedures
  - 4.1. Determining information classification
  - 4.2. Research data
  - 4.3. Educational data and learning analytics
  - 4.4. Digital information service classification
  - 4.5. Handling “Public” and “Internal Use Only” information
  - 4.6. Handling “Restricted” and “Highly Confidential” information
  - 4.7. Information reclassification

### 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

<b>Public Information</b>	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.
<b>Internal Use Only Information</b>	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.
<b>Restricted Information</b>	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 Examples include student records or analytics data, staff records, unpublished research reports or data, audit reports and Council papers.
<b>Highly Confidential Information</b>	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.

<b>Digital Information Service</b>	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.
<b>Information Asset</b>	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.

<b>Determining “Public” Classification</b>	<ul style="list-style-type: none"> <li>a. The information or service is specifically for public access (e.g. Flinders website, or research that has been released); and</li> <li>b. No adverse impact to University resulting from publication (or such publication is specifically approved).</li> </ul>
<b>Determining “Internal Only” Classification</b>	<ul style="list-style-type: none"> <li>c. The information is not for public access; and</li> <li>d. Accidental or deliberate disclosure or unauthorised access to the information would result in minor or no adverse impact to the University.</li> </ul>
<b>Determining “Restricted” Classification</b>	<ul style="list-style-type: none"> <li>e. The information is for limited distribution to specific groups within the University; and</li> <li>f. Contains research data, educational data, financial data, strategic information or personally identifiable data; and</li> <li>g. Accidental or deliberate disclosure or unauthorised access to the information results in modest financial, reputational and/or legal impact to the University.</li> </ul>
<b>Determining “Highly Confidential” Classification</b>	<ul style="list-style-type: none"> <li>h. The information is for very limited distribution to specific individuals within the University; and</li> <li>i. Contains research data, financial data, strategic information or personally identifiable data; and</li> <li>j. Accidental or deliberate disclosure or unauthorised access to the information results in critical financial, reputational and/or legal impact to the University.</li> </ul>

### 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

<b>Labelling</b>	No specific requirement to label information at this classification level, unless likely to be accessed by third parties.
<b>Cloud/Network Storage</b>	<ul style="list-style-type: none"> <li>• Network storage does not require access restrictions beyond a limitation to users with a Flinders FAN account;</li> <li>• Internet-based (“cloud”) file storage is allowed for approved providers.</li> </ul>
<b>Portable Storage</b>	Storage on portable storage devices is allowed without restrictions.
<b>Hard Copy Storage</b>	No restrictions for printed storage.
<b>Email Restrictions</b>	No restrictions for information included as email attachments.
<b>Access by University Personnel</b>	No access restrictions for University personnel.
<b>Access by External Parties</b>	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

<b>Labelling</b>	Documents should include label “Restricted” or “Highly Confidential”, as appropriate, in header or footer of each page.
<b>Cloud/Network Storage</b>	<ul style="list-style-type: none"> <li>• Limit network storage access to authorised <b>groups</b> only (for Restricted documents/data) or authorised <b>individuals</b> only (for Highly Confidential documents/data);</li> <li>• Internet-based (“Cloud”) hosting permitted for Restricted documents, but only for approved storage providers;</li> <li>• Highly Confidential information should <b>not</b> be stored on Cloud storage services.</li> </ul>
<b>Portable Storage</b>	Encrypt all information on portable storage devices.
<b>Hard Copy Storage</b>	Store within secure closed container, which can include a locked cabinet or locked office.
<b>Email Restrictions</b>	Encrypt documents or data before attaching to any email message.
<b>Access by University Personnel</b>	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

<b>Approval Authority</b>	Vice-President (Corporate Services)
<b>Responsible Officer</b>	Chief Information Officer
<b>Approval Date</b>	21 December 2017
<b>Effective Date</b>	21 December 2017
<b>Review Date*</b>	December 2020
<b>HPRM file number</b>	CF18/18

\* Unless otherwise indicated, this procedure will 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.