Information Classification

Quick Reference Guide – Document Handling

The Classification Scheme enables Flinders University to identify categories of information that are of the same value in terms of impact if lost or disclosed to unauthorised parties. This quick reference guide describes the handling procedures for each classification category.

	Highly Confidential	Restricted	Internal Use Only	Public
Definition	Information containing personally identifiable information, research or enterprise 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: Medical records, Council papers, WorkCover claims.	Information containing personally identifiable information, research or enterprise data that if released could result in ***modest*** financial, reputation or legal impact to the University or an affiliated organisation or individual. Examples: Audit reports, intellectual property, student/ staff records.	Information considered internal to Flinders University that is not generally publically available. Disclosure could cause ***minor or no*** impact to the University or an affiliated organisation or individual.. Examples: day-to-day emails, procedures, project and other administrative documents.	Information that is in the public domain or that has been approved for release to the general public. Examples: Student course information, staff contact information, marketing and brochures, approved media releases, website content.
Labelling Requirement	**Must** be labelled "Highly Confidential" in the header or footer of each page	**Must** be labelled "Restricted" in the header or footer of each page	**Should** be labelled with "Internal Use Only" in the document header or footer If sending outside the University. Otherwise, no requirement to label.	No requirement to label
Cloud/Network Storage	**Must** be stored in a folder with access to authorised individuals only. Internet-based ('cloud') hosting NOT permitted.	Must be stored in a folder with access to authorised groups only. Internet-based ("cloud") hosting permitted after review by ITS Security Services.	No restrictions for internal storage. Internet-based ("cloud") hosting permitted.	Internal and external hosting allowed without restriction.
Portable Storage	Device/file **must** be **ENCRYPTED** Contact ITS Security Services for guidance if necessary	Device/file **must** be **ENCRYPTED** Contact ITS Security Services for guidance if necessary	Allowed without restriction, however handle and store the device in the same fashion as hardcopy records	Allowed without restriction
Hardcopy Storage	Store within a secure closed container this includes locked cabinet or locked office	Store within a secure closed container this includes locked cabinet or locked office	**Should** be stored in suitable containers such as bookcases, drawers or cabinets	Allowed without restriction
E-mail	If information is sent externally it **must** be ENCRYPTED Contact ITS Security Services for guidance if necessary	If information is sent externally it **must** be ENCRYPTED Contact ITS Security Services for guidance if necessary	Allowed without restriction	Allowed without restriction
External Access	A formal confidentiality agreement **must** be signed by the third party prior to information being exchanged	A formal confidentiality agreement **must** be signed by the third party prior to information being exchanged	The information Owner **must** approve the release of information to third parties	As approved by Marketing and Communications Office (For release to Public)

For further guidance please refer to the **Information Classification Framework** or contact **ITS Security <ictsecurity@flinders.edu.au>**