Information Handling Guidelines

1. An Information Classification Policy has been created and covers all information and data held by the University in any format, both electronic and hardcopy. It consists of 4 categories: Public, Internal, Sensitive and Confidential and applies to all users of University information and data; staff, student and externals.

2. These guidelines give advice on how information in each category of information should be retained, handled and stored. These also apply to all users of University information and data; staff, student and externals.

3. The guidelines cover information in all forms – both digital and physical.

4. It is permitted to access all types of information from any device in any location using University supplied remote access systems (e.g. RDS).

5. Before sharing or storing any information, consideration must be given to its probable classification and therefore whether this is permitted. Anyone using University information has personal responsibility for conforming to the policy and these guidelines.

6. The table below gives broad advice on how different types of information should be stored and transmitted.

7. If in any doubt, refer either to the information owner or a senior manager.

8. A department may wish to have other approved procedures for labelling and handling sensitive and confidential information because of the nature of their work. Any guidelines created by an individual department must have those guidelines approved, in writing, by the University Solicitor's department.

9. Allegations of infringement of these guidelines may constitute a disciplinary offence under the applicable process for members of staff or students.

Information Handling Guidelines

Guidelines on how the different classifications of information should be stored and transmitted

Note that where it is stated below "University only", this can include sharing with partner colleges as long as it is only information concerning students at that partner.

Handling issue	Public	Internal	Sensitive	Confidential
Electronic Storage Location: University Approved (eg N: drive, department share, Onedrive for Business)	No restrictions	No restrictions	No restrictions, but care needed on sharing and access rights	Allowed only if sharing, user access and synchronization have been reviewed and are appropriate
Electronic Storage Location: Other (eg personal cloud storage, DropBox, iCloud etc)	No restrictions	Not allowed	Not allowed	Not allowed
Webpages	No restrictions	Internal University webpages only	Not allowed	Not allowed
Electronic Storage Protection (eg Encryption, access control, authentication and authorisation)	Unprotected	Basic password authentication or similar	Validated strong passwords or similar	Strong authentication and encryption
Mobile devices (eg laptops, tablets, smartphones)	No restrictions	No restrictions	Device must be encrypted or password protected	Not recommended, allowed with information owner's explicit permission only, must be suitably protected
Portable or removable storage (eg flash memory cards, USB sticks, portable hard drives)	No restrictions	No restrictions	Not recommended, device or information must be encrypted	Not recommended, allowed with information owner's explicit permission only, must be encrypted
Physical Storage (eg desks, shells, filing cabinets)	No restrictions	Take reasonable precautions	Store carefully so as to restrict access to authorized people	Store in a locked container; restrict access to authorized people

Handling issue	Public	Internal	Sensitive	Confidential
Electronic Transmission (eg email, file transfer, web upload)	No restrictions	Care taken to verify recipient	Internal only **or** Encrypted / secure if to external	Internal to University **or** by agreement with information owner only and with strong encryption
Faxing (eg sending a copy by electronic facsimile to another organisation or person)	No restrictions	Take reasonable precautions to restrict access and confirm delivery to recipient	Restrict access to sending machine during transmission, and notify recipient to stand by for receipt of fax and confirm delivery	Restrict access to sending machine during transmission, and notify recipient to stand by for receipt of fax and confirm delivery
Copying – physical (eg scanning, photocopying or photographing a copy of the information)	No restrictions	In-house copying preferred. If outside copying is used, original should be returned to the University	In-house copying required; shred spoils or overruns	With agreement o information owner only. In-house copying required; securely shred spoils or overruns
Copying – electronic (eg creation of additional versions of files or documents, possibly in other electronic locations)	No restrictions	No restrictions	Permitted, but with care	With explicit agreement of information owner only.
Destruction Method – physical (eg waste disposal of physical paper copies)	Any	Place in proprietary waste	Shred into strips or place in confidential waste bin	Cross-cut shred into small pieces
Destruction method – electronic (eg removal of an electronic copy of a document or file)	Delete	Delete	Delete and remove from waste bin or similar	Use secure deletion tools to wipe from disk and computer memory.

Handling issue	Public	Internal	Sensitive	Confidential
Labeling (eg watermarks, stickers, stamps, titles, folders, filenames)	Not required, optional if helps clarity	Not recommended	May label electronic information with watermark if desired	Recommended to label electronic with watermark, in document name or in document itself and physical with designation on cover

Document control					
Version	**Author(s)**	**Owner**	**Date Approved**	**Approved by**	**Review date**
1	IE and working group	IT	7 May 2016	ITSPG	May 2017