Information Classification Policy

Purpose

The purpose of this policy is to provide a system of categorising information in relation to its sensitivity and confidentiality and to define expected processes for the handling of each classification of information. This is in the interests of providing suitable confidentiality and protection of the information.

Scope

What information does the policy apply to? The policy applies to all information held by the University both in electronic and hard copy formats.

Who does the policy apply to? All staff employed by the University, external examiners, consultants and other casual employees of the institution are required to take personal responsibility for ensuring appropriate care is taken to ensure information is handled in line with the policy to uphold security and confidentiality of the information. The policy also applies to students when using personal or sensitive data for research and other academic work.

Policy

The policy includes the following classifications of information;

- **Unclassified** – information that is freely in the public domain and to which no access controls are required.
- **Restricted** – information that is unlikely to harm the University or individuals if disclosed but is restricted for internal use and publication.
- **Confidential** - Information that has potential to cause some negative impact to individuals or to the University's commercial or reputational interests if released. This includes personal data that enables individuals to be identified.
- **Highly Confidential** - Information that is likely to cause serious impact to individuals or to the University's commercial or reputational interests if released. This includes sensitive personal data as well as commercially sensitive information.

In most cases personal data or commercially sensitive data will fall into either the confidential or highly confidential classification and more stringent controls need to be placed on storage mediums and disclosure of the data.

Individuals are required to assess the sensitivity of information being created or received and take appropriate steps to ensure it is kept secure. Guidance is provided in **Annex A and B** to assist with determining the most appropriate information classification and outline key controls for protecting the data. Further assistance should be sought from a line manager where there may be doubt about how to proceed with classifying information. IT Services should be consulted if guidance is needed on the appropriate security of storage mediums.

Where confidential or highly confidential information is shared with other colleagues within the University it should be clear to all recipients what the classification of the information is through appropriate labelling.

Evaluation and review

This policy will be formally reviewed every year by the Data Protection Officer and the relevant department(s) within the University. In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

This policy was last updated in June 2021.

Annex A – Guidance on Assessing Appropriate Information Classification

Classification Name	Unclassified	Restricted	Confidential	Highly Confidential
Summary Description	**Information that is freely available in the public domain**	**Information that would not likely do any harm to the University or individual staff or students if released but is restricted for internal publication only.**	**Information that has potential to cause some negative impact to individuals or to the University's commercial or reputational interests if released**	**Information that is likely to cause serious impact to individuals or to the University's commercial or reputational interests is released.**
Key examples of information in these categories (not exhaustive)	Information the public would generally expect to find on the University website such as current courses, fees, student services offered, University strategy documents.	Internal analysis of information available publicly that may include commentary or opinion the University would not wish to make public.	Information that enables identification of individuals and private information about them, but not highly sensitive personal data.	Highly sensitive personal data about individuals (students, staff and data collected from research subjects).
	Information the University routinely publishes as part of marketing and promotional materials such as the prospectus.	Information that is intended for staff use only such as operating procedures.	Individuals' names with home contact information, age, date of birth, student or staff ID numbers; including data about research subjects.	Financial information such as payment details from bank accounts and credit cards (only held on bespoke systems for this data).
	Publicly available staff directories including names, job titles, work phone and email details and departmental information.	Not containing any personal information to identify individuals or commercially sensitive information.	Attendance details of students.	Information on individuals' ethnic origin, religious beliefs, disability, physical and mental health records, criminal records.
	Information contained within corporate annual reports.		Exam marks.	Disciplinary information (students or staff).
	Available publicly from other organisations such as HESA, HEFCE or UCAS.		Comments or transcripts about performance.	References for staff or students where highly sensitive content is being provided such as information related to health or disciplinary matters.
	Final degree classification.		References for staff or students where no highly sensitive content is being provided such as information related to health o disciplinary matters.	Critical information about the University's commercial interests such as planned new provision, fees, recruitment data, funding and research bids that is not in the public domain.
			Information about the University's commercial interests not in the public domain (although not deemed of critical importance to maintain secrecy).	Intellectual property rights.
			Employee contract information.	University contracts and supplier information.
			Unpublished research papers.	

Annex B – Appropriate Storage and Protection of Classified Information

Classification Name	Unclassified	Restricted	Confidential	Highly Confidential
Summary Description	**Information that is freely available in the public domain**	**Information that would not likely do any harm to the University or individual staff or students if released but is restricted for internal publication only.**	**Information that has potential to cause some negative impact to individuals or to the University's commercial or reputational interests if released**	**Information that is likely to cause serious impact to individuals or to the University's commercial or reputational interests is released.**
Access Controls Required	No restrictions	Staff only.	Limited to staff requiring access to the systems where the information is held.	Only staff in a role requiring specific access o the information. This should be restricted as tightly as possible on an individual basis.
Appropriate University systems to store data	No restrictions	Systems requiring access through a University account.	Personal Storage area (e.g. My Documents/ Y:) on University Network Drives, on University shared network drive or the OneDrive for Business. If the file is stored on a shared network drive or in OneDrive for Business, you should ensure that access to that file is restricted only to those who require access	Personal Storage area (e.g. My Documents/ Y:) on University Network Drives, on University shared network drive or the OneDrive for Business. If the file is stored on a shared network drive or in OneDrive for Business, you should ensure that access to that file is restricted only to those who require access.
University approved cloud storage (OneDrive for Business)	No restrictions	No restrictions	Permitted as the University's use of OneDrive is encrypted in transit and at rest. Extreme caution should be exercised to ensure files are placed in OneDrive folders accessible only by appropriate staff.	Permitted as the University's use of OneDrive is encrypted in transit and at rest. Extreme caution should be exercised to ensure files are placed in OneDrive folders accessible only by appropriate staff.
University OneDrive for Business synchronised local folders	No restrictions	No restrictions	Permitted but only on a device owned and encrypted by the University. Not permitted to be stored on synced located on any other devices.	Permitted but only on a device owned and encrypted by the University. Not permitted to be stored on synced located on any other devices.
Private cloud storage accounts e.g. Dropbox, Icloud, GoogleDrive, OneDrive on personal email accounts	No restrictions	Not permitted	Not permitted	Not permitted
USB memory sticks	No restrictions	Yes, but must be a device that has been encrypted by IT Services to University approved standards.	Yes, but must be a device that has been encrypted by IT Services to University approved standards.	Yes, but must be a device that has been encrypted by IT Services to University approved standards.
Remote access to information	No restrictions	No restrictions	Only through University approved remote access provision.	Only through University approved remote access provision.
Storage on University owned mobile devices	No restrictions	Yes, but must be a device that has been encrypted by IT Services to University approved standards.	Yes, but must be a device that has been encrypted by IT Services to University approved standards.	Yes, but must be a device that has been encrypted by IT Services to University approved standards.
Storage on privately owned devices (not using OneDrive for Business synchronised folders)	No restrictions	Not permitted	Not permitted	Not permitted
Sending data by internal email	No restrictions	No restrictions	Only to recipients with a clear operational need to receive the information.	Only to recipients with a clear operational need to receive the information.
Paper copies	No restrictions	No restrictions	Only where explicitly required for operational reasons and to be kept in a locked filing cabinet or equivalent.	Only where explicitly required for operational reasons and to be kept in a locked filing cabinet or equivalent.

Classification Name	Unclassified	Restricted	Confidential	Highly Confidential
Summary Description	**Information that is freely available in the public domain**	**Information that would not likely do any harm to the University or individual staff or students if released but is restricted for internal publication only.**	**Information that has potential to cause some negative impact to individuals or to the University's commercial or reputational interests if released**	**Information that is likely to cause serious impact to individuals or to the University's commercial or reputational interests is released.**
Circumstances in which external parties may have information disclosed	No restrictions	where the University chooses to provide to further its own interests or to collaborate with other organisations such as press releases or to support tenders or bids.	Only where the University is legally obliged to do so through obligations to regulatory bodies (such as HESA and funding councils) or from specific use of Data Protection Act exemptions such as disclosures to the Police investigating a criminal offence.	Only where the University is legally obliged to do so through obligations to regulatory bodies (such as HESA and funding councils) or from specific use of Data Protection Act exemptions such as disclosures to the Police investigating a criminal offence.
Requirement for transfer of data externally	No restrictions	No restrictions	Through secure extranet facilities compelled by regulatory bodies or through secure OneDrive sharing where adhoc exceptions have been made.	Through secure extranet facilities compelled by regulatory bodies or through secure OneDrive sharing where adhoc exceptions have been made
Sending data by external email	No restrictions	Permitted, but must advise the recipient that the material is not for onward disclosure; mark as "in confidence".	Where adhoc exemptions have been appropriately made this can be done, but secure OneDrive sharing must be used to send the information,	Where adhoc exemptions have been appropriately made this can be done, but secure OneDrive sharing must be used to send the information,