Data Classification and Handling Guidance

1. Purpose

This guidance provides a framework for classifying and handling data to ensure that the appropriate degree of protection is applied to all data held by the University. The classification of data will help determine how the data should be accessed and handled and ensure that sensitive and confidential data remains secure.

The correct classification of data is important to help ensure the prevention of data leaks and minimising the impact of such leaks if they do occur. As well as being good practice, it will also help ensure the University remains compliant with the requirements of the Data Protection Act 1998 (or the General Data Protection Regulations (GDPR) from 25th May 2018) and ensure effective handling of Freedom of Information requests.

This guidance will explain the responsibilities of individuals and provide a consistent classification scheme to ensure that data is appropriately protected and managed throughout the University.

2. Scope

This guidance covers all data or information held, in physical or electronic format, by the University including documents, spreadsheets and other paper and electronic data and should be applied by all staff, students and other members of the University. Appendix A includes a definition of data.

This guidance is also applicable to associates working with the University, agency staff, data processors, third parties and collaborators working with the University. They are responsible for assessing and classifying the information they work with and applying appropriate controls. Members of staff working with these types of associates and third parties have a responsibility to bring this guidance to their attention.

3. Categories

Data classification is based on the level of sensitivity and the impact on the University should that data be disclosed, altered, lost or destroyed without authorisation. The classification of all data into different categories ensures that individuals who have a legitimate reason to access a piece of information are able to do so, whilst at the same time ensuring that data is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required to be in place.

All data owned, used, created or maintained within the University should be categorised into one of the following four categories:

- Public
- Sensitive
- Confidential
- Secret

The majority of information held by the University will come under Public and Confidential categories. A smaller amount of information will be categorised as Restricted. The secret classification is only to be used in exceptional circumstances.

The table below (appendix 1) provides details on the types of information which come into each of these categories, who should have access to this information, how the information should be stored, transmitted and the methods of disposal that can be used.

4. Responsibility and Ownership

All data and information must be held in an information asset and therefore would be included in the Information Asset Register held by each Directorate/Department and Faculty/School. The Information Assets are the responsibility of the Information Asset Owner (IAO) who is the Director/Dean of each and every Directorate/Faculty. The IAO's will be supported by Information Asset Managers (IAM) and Administrators (IAA) where required.

Information security is everyone's responsibility and therefore all members of the University have a responsibility to protect University data and information. All university members should have an awareness of the four data classifications and the way in which the data and information in each classification should be handled.

5. Removal of Information Assets

Staff/Student(s) of the University must not remove sensitive information assets (Confidential/Strictly Confidential/Secret) from the University premises without the prior agreement or consent from an appropriate authority. In the event of authorised removal of information assets, it is your responsibility to adequately protect the information assets at all times and to return them in the condition in which they were originally provided to you.

6. Secure Disposal

Information assets which are considered sensitive (i.e. Secret, Confidential or Restricted), and are no longer needed or are deemed to have reached "end of life" must be securely disposed of. There are several ways to dispose of information assets and equipment. These include:

Secure shredding (Cross cut shredders)

The University has a number of shredders which should be used to ensure secure disposal of all confidential information assets that are no longer needed. This removes the need for Staff/Student(s) of the University to store unwanted information assets. If sensitive data is shredded then a cross-cut shredder is recommended.

Confidential waste disposal bins (Paper based)

Confidential waste bins are available within many University departments and are an alternative to secure shredding.

Appendix A - Data Classifications and Handling requirements

	Public	Confidential	Sensitive	Secret
Impact if the information was made public	**None**	**Low** May result in minor reputational or financial damage to the University; May result in minor privacy breach for an individual	**Medium** Could substantially damage reputation of the University. Have a substantial financial effect on the University or a third-party, Would result in a serious privacy breach to one or more individuals	**High** Inappropriate disclosure could cause significant damage to the University's reputation or operations, great distress to individuals, pose a danger to personal safety or to life or impede the investigation or facilitate the commission of serious crime; substantial financial or legal penalties
Description	Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with the University or not. Information is likely to already exist in the public domain.	May result in very minor reputational or financial damage to the University; May result in very minor privacy breach for an individual Information that should only be available to sub-groups of staff within the University who need access to the information to carry out their roles.	Information that has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive or legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.	Access is subject to or obtained under the Official Secrets Act or equivalent or data that, if inappropriately accessed could cause catastrophic harm to the University, staff and the data subjects This data should be secured on separate disc drives with very strict access controls in place.

Examples (please note the list is not exhaustive)	• Prospectus, programme and course information. • Press releases not under embargo. • Open content on the University web site. • Flyers and publicity leaflets • Published information released under the Freedom of Information Act. • Annual report and financial statements. • Job adverts (excluding internal only positions) • Faculty names codes and addresses. • Programme, unit and school/department names. • Staff publications. • Agendas and minutes of University committees and working groups (minus any reserved business). • Patented intellectual	• Student personal details e.g. demographics, student number, personal email address etc. • Staff personal details e.g. demographic, payroll number, personal email address etc • Internal only University policies, processes and guidelines. • Internal only job adverts. • Tender bids prior to award of contract • Individual's salaries • Student's assessment marks. • Job application responses/CVs (unless these contain Sensitive Personal Information (as defined in Appendix C).	• Sensitive personal data (as defined in Appendix C) • Exam questions prior to use • "On-going" research papers • Medical records • Usernames and passwords • Investigations/disciplinary proceedings. • Payment card details. • Financial information such as bank account details. • Financial data (that not disclosed in financial statements). • Passwords and access codes to University systems. • Press releases under embargo. • Research Participant Contact Details • Medical information regarding research participants • Research participant complaints/requests relating to their	• Access is subject to or obtained under the Official Secrets Act or equivalent obtained as part of a research project

	property.		participation • Donor identification data attached to a human sample	
Security Marking	No marking required	Must be clearly marked as Confidential	Must be clearly marked as Sensitive	Must be clearly marked as Secret
Storage (Electronic)	Electronic information should be stored using Keele IT facilities to ensure appropriate management, back-up and access. **Dropbox** must not be used as it links to C: drives on PC/Desktops etc which is not secure. Google Drive File Stream will connect to your Google Drive and not require IT to give write access to the C: Drive. It comes with benefits of better integration with Keele systems and email. Better security is provided by Google as it warns users that they are about to share data with someone outside of the organisation. Dropbox will not provide this. We would like all users to move to Google Drive on the managed desktop so they can be managed more easily.	Must not be stored in any personal cloud storage solution such as Dropbox (see explanation in the Public column) or on local drives (e.g. C: drive on local computers unless your PC/Laptop is on the Domain in which case your My Documents and Download folders only are stored on a network drive and therefore secure). Please be aware that if your PC/laptop is not on the Domain there is a risk when downloading a file (e.g. from KLE or Google Drive) that it could end up on your C: drive which is not secure therefore ensure that you download to an appropriately secure network drive. Portable devices such as USB sticks cannot be used for long term storage and must be encrypted. A portable USB hard drive can be used but should not be seen as a long-term solution due	Must be stored on the University network in restricted access drives which only those authorised to access the data have access to. If particularly sensitive consider encrypting the document as well. Can be stored in Keele Google Drives however a security copy should also be kept on the University secure network drive with limited access. Do not store on personal Google drives. Must not be stored in any personal cloud storage solution such as Dropbox (see explanation in the Public column) or on local drives (e.g. C: drive on local computers unless your PC/Laptop is on the Domain in which case your My Documents and Download folders only are stored on a network drive and therefore secure). Please be aware that if	Must be stored only on the University network in rigorously monitored restricted access drives which only those authorised to access the data have access to. These drives must be located on the University's central network. Must not be stored in Keele or personal Google Drives If particularly sensitive consider encrypting any documentation as well. Must not be stored in any personal cloud storage solution such as Dropbox, on local drives (e.g. C: drive on local computers) or on portable devices such as USB drives.

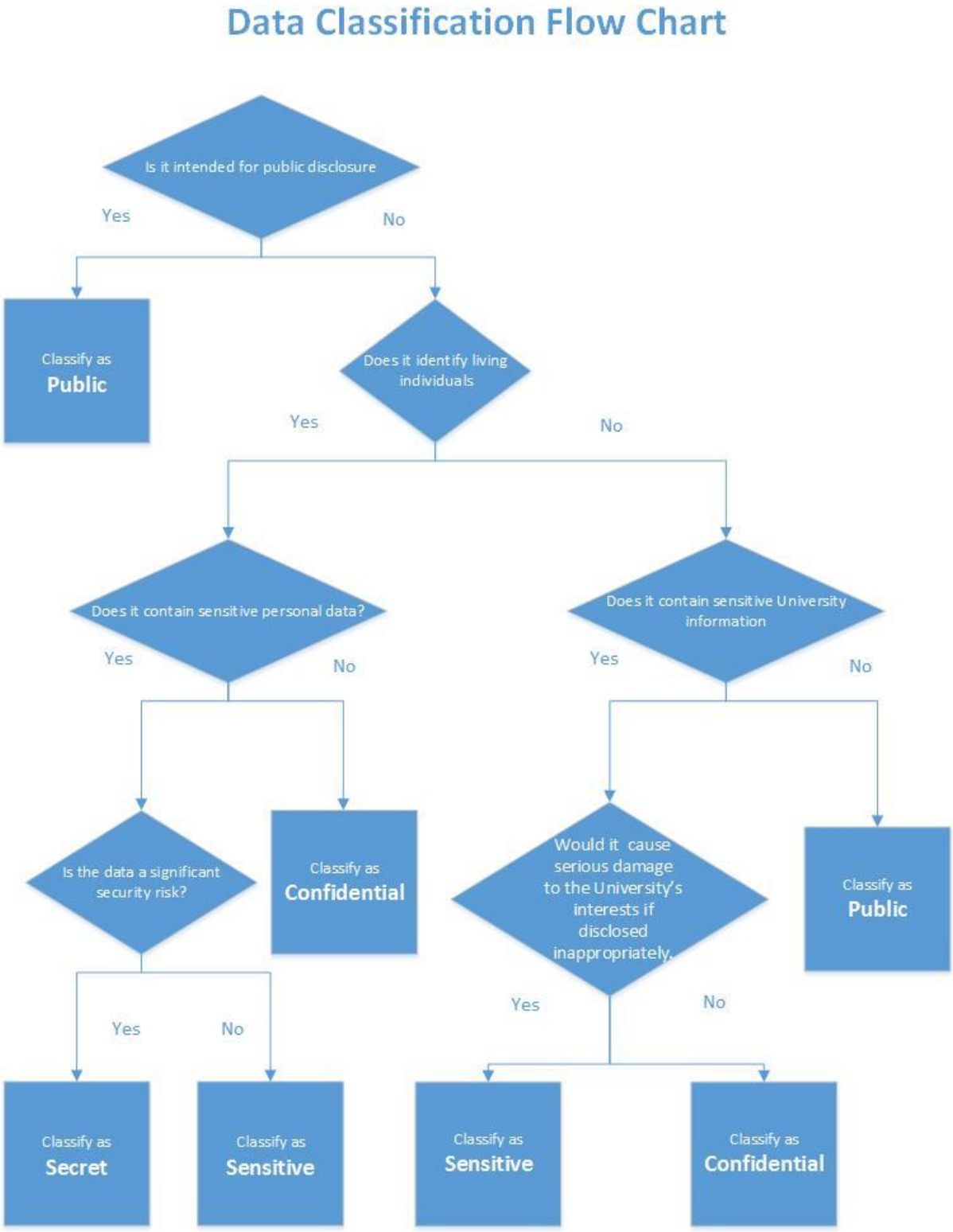
		to risks of loss for example. The drive must be encrypted. Can be stored on network or Keele Google Team drives as long as the Team Drive is shared with an appropriate person. Do not store on personal Google drives. Portable devices including laptops, iPads and USB hard drives must be fully encrypted.	your PC/laptop is not on the Domain there is a risk when downloading a file (e.g. from KLE or Google Drive) that it could end up on your C: drive which is not secure therefore ensure that you download to an appropriately secure network drive.. Portable devices such as USB sticks cannot be used for long term storage and must be encrypted. Portable devices, including laptops and iPads must be fully encrypted. Passwords may be stored in online password vaults or managers however the password to these applications must adhere to the strong password management guidance	
University Website	No Restrictions	Not permitted	Not permitted	Not permitted
Storage (hardcopy)	No restrictions	In a lockable cabinet or drawer which is locked when the office is left unattended and also locked	In a lockable cabinet or drawer which is locked when office is left unattended and also locked. If hard-copies are stored on shelving within a lockable room then this room should be locked at all times when unattended and must have restricted	Preferably no hard copy should exist for storage. Where possible, all documentation should be scanned and stored electronically. If this is not possible, store in a lockable cabinet or drawer which is locked when office is left unattended and also

			access.	locked.
Email (University Hosted Gmail)	Yes	For emails to external recipients must be put in an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone call to or from the recipient. For emails to internal recipients i.e. Keele email account to Keele email account, encrypted attachments are not necessary.	For emails to external recipients must be put in an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone call to or from the recipient. For emails to internal recipients i.e. Keele email account to Keele email account, encrypted attachments are not necessary.	Must not be emailed and should only be transmitted electronically in an acceptably encrypted format or through secure FTP.
Email (Personal internet based email accounts e.g. Hotmail)	Yes	Not permitted	Not permitted	Not permitted
Post (Internal)	Yes	In sealed envelope marked confidential.	In sealed envelope marked Confidential and hand delivered.	In sealed envelope marked Highly Confidential and hand delivered.
Post (External)	Yes	Tracked and recorded delivery only and marked confidential	Tracked and recorded delivery only and marked confidential within two separate envelopes.	Tracked and recorded delivery only and marked highly confidential within two separate envelopes.
School or Department based server	No restrictions but consideration should be made to back-up requirements	No storage or creation permitted unless server environment is equivalent to IT or CTU server environment.	No storage or creation permitted unless server environment is equivalent to IT or CTU server environment.	No storage or creation permitted unless server environment is equivalent to IT or CTU server environment and approved by IT
University owned laptop	Do not use to store master copies of vital records.	Laptop must have the internal storage (hard drive(s), HDDs, SSDs) encrypted. Device set to lock after five minutes of	Laptop must have the internal storage (hard drive(s), HDDs, SSDs) encrypted. Device set to lock after five minutes of	Laptop must have the internal storage (hard drive(s), HDDs, SSDs) encrypted. Device set to lock after five minutes of

		inactivity.	inactivity.	inactivity.
Personally owned mobile devices	Yes	Must only be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the BYOD guidance document.	Not permitted unless SIRO authorisation. Must only be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the BYOD guidance document.	Not permitted
University owned desktop in public areas	Yes, lock screen when unattended	Not permitted. *High risk of incidental disclosure*	Not permitted. *High risk of incidental disclosure*	Not permitted. *High risk of incidental disclosure*
University owned desktop in non-public areas i.e. there is restricted and controlled access to the building e.g. swipe card or keypad access control system	Yes, lock screen enabled when the desktop is left unattended	Encrypt Drive or password protect files Lock screen when unattended	Encrypt Drive Lock screen when unattended	Encrypt Drive Lock screen when unattended
University owned mobile devices	Yes	Must only be stored on devices that are encrypted and have PIN/password/Biometric access controls applied and in line with the Mobile Device guidance document.	Not permitted unless SIRO authorisation. If authorisation given must only be stored on devices that are encrypted and have PIN, password or Biometric access controls applied.	Not permitted unless SIRO authorisation. If authorisation given must only be stored on devices that are encrypted and have PIN/password/Biometric access controls applied.
Removable Media	No restrictions	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase,	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase,	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase,

		digits and special characters.	digits and special characters.	digits and special characters.
Disposal	No restrictions. Recycle where possible	Shredding or use confidential waste bags. Delete from electronic media when no longer required	Cross shredding only then the shredded material must be put into confidential waste bags. Ensure electronic media is wiped clean. If encrypted USB stick has been used then send to IT Dept. for secure destruction	Cross shredding only then the shredded material must be put into confidential waste bags. Ensure electronic media is wiped clean. If encrypted USB stick has been used then send to IT Dept. for secure destruction

Appendix B



Version number:	Final v1.0	Approval:	By Date	UEC 20th February 2018	Owner:	RIE and IT	Review Date:	19/02/2019	Author: S. Clements Information Security Manager

Appendix C

General Data Protection Regulations Definitions

1. **"Personal data"** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

2. **"Sensitive Personal Data"** are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).