Data Classification Schedule

Enquiries relating to this document - legal@uws.ac.uk

Purpose

This document provides the framework for classifying and handling UWS data ensuring appropriate degrees of protection are applied to all data held by the University. The classification of data will help determine how data should be accessed, handled and stored, ensuring that sensitive and confidential data remains secure. The correct classification of data is an important to help ensure the prevention of data loss and minimising the impact of such losses if they do occur.
As well as being good practice, it will also help ensure the University remains compliant with the requirements of the UK General Data Protection Regulation and the UK Data Protection Act (2018). This policy will explain the responsibilities of individuals and provide a consistent classification scheme to ensure that data is appropriately protected and managed throughout the University.

Scope

This policy covers all data or information held, in print or in electronic format, by the University including documents, spreadsheets and other paper and electronic data and should be applied by all staff and partners of the University including agency staff, data processors, third parties and any other external collaborators. They are responsible for assessing and classifying the information they work with and applying appropriate controls. Members of staff working with partners and third parties have a responsibility to bring this data classification schedule to their attention.

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 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 provides guidance on the appropriate security and technical controls to have in place.

All data owned, used, created or maintained within the University should be categorised into one of the following four categories: Public (P), Restricted (R) Confidential (C1) and Strictly Confidential (C2). The majority of information held by the University will come under the Public and Restricted categories. A smaller amount of information will be categorised as C1 or C2. The table below provides details on the types of information which come into each of these categories, who should have access to this information, how and where the information should be stored or transmitted and the methods of disposal that should be used.

Responsibility and Ownership

All data or information should have an owner. This could be the author of a document or the School/Division or Service area responsible for the data. It is acknowledged that it is not feasible to mark every single document in the University with the appropriate data classification, however, it is the responsibility of all members of University staff to have awareness of the four data classifications and the way information within each category should be handled. For the majority of information it is likely to be obvious by its nature which category it should come within. Where there is a possibility of ambiguity over the status of the document it is the responsibility of the data owner to ensure that the document or data is clearly marked and/or they make anyone who has access to the information aware of its status. This is particularly the case for

C1 and C2 information which should where practicable be marked. Whilst this in itself does not make the information secure it assists with appropriate information handling. All members of the University have a responsibility to protect University data.

The following refers to both electronic and hard copy data.

	Data Classification			
	Public (P)	**Restricted (R)**	**Confidential (C1)**	**Strictly Confidential (C2)**
Impact if information Made Public	**None**	**Low** **Minor reputational or financial damage to University** **Potential minor privacy breach for an individual**	**Medium** **Intermediate reputational, financial, legal or privacy impact.** **May impact on the trust reputation of University in future.** **Breach of personal information belonging to several individuals which may cause distress to those individuals**	**High** **Substantial damage to reuputation of University or substantial financial loss to UWS or partner.** **Breach of personal information belonging to significant number of individuals**
Definition	*Information that is publicly available or in the public domain or where confidentiality would have no particular significance. This information does not require protection and may be seen by anyone whether directly linked to the University or not.*	*Non-confidential information intended for internal use only, but if compromised or destroyed, would not have a catastrophic impact on the University or individuals. Inappropriate disclosure would have minimum significance however consideration should be given to appropriate security of data.* *Normally available to all UWS staff members although access may require to be limited to specific groups.*	*Information which is sensitive in some way. It may be personal data, commercially sensitive, legally privileged, or under embargo prior to being released at an approved time. Normally only available to specified authorised UWS staff members, using password control etc.*	*Special Category data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation* *Criminal convictions or alleged offences Individuals' financial information including credit card/bank account details. Exam questions prior to use*

Description/Examples	Publications including prospectus/leaflets, course information Press releases. Policies/Procedures Anonymised statistics. Public web content. Published information released under the Freedom of Information (Scotland) Act 2002. Can include personal data where an individual has consented for it to be used publically, for example, on social media.	Committee minutes where not marked 'confidential'. Departmental Intranet/Connect content. University timetable. On-line directory of contact details. Teaching materials. Exam papers post use. Procurement documents not relating to tender review process. Copies of Emails that do not contain confidential data Lists of staff names, qualifications and e-mail addresses.	Documents which contain identifiable personal information e.g. address/telephone number/date of birth/National Insurance Number. HR Data such as an employment contract Student data including transcripts Student attendance details. Exam marks. Wage slips Commercial contracts Copies of emails containing confidential data Financial information not disclosed in publicly available financial statements. Procurement card data. Reserved Committee business Internal audit reports. Procurement tender review docs and staff evaluation comments. Tender responses, methodology and pricing which may contain intellectual property.	Financial data Examination papers pre use Medical records Certain medical research data Research papers intended to lead to patentable results (If research is ongoing and has not been published) – Certain commercial contracts containing market sensitive information. Details of servers and server rooms – Passwords Copies of emails containing strictly confidential data or special category data. Investigations/disciplinary proceedings - Market sensitive information (e.g. concerning some property purchases). Legally privileged information
Security Controls	No Encryption required. Should be deleted/disposed of when no longer required in line with data retention schedules. Consideration given to backup and staff leaver handover.	Encryption, staff leaver and back up requirements should be considered. Should be deleted/disposed of when no longer required in line with data retention schedules (unlikely to require shredding)	**Electronic Files** - should be encrypted using password protection*****. Owner and line manager must be aware of backup processes and requirements for handover in event of leaving UWS. Files should be deleted in accordance with data retention schedules. **Hard copies** - shredded when no longer required in accordance with data retention schedules Tracked/"signed for" mail for external or double envelope for internal	**Electronic Files** - should be encrypted using password protection*****. Owner and line manager must be aware of backup processes and requirements for handover in event of leaving UWS. Files should be deleted in accordance with data retention schedules. **Hard copies** - shredded when no longer required in accordance with data retention schedules Tracked/"signed for" mail for external or double envelope for internal
Can be Stored in	UWS Shared Drives UWS OneDrive DropBox/Google Drive etc. USB Drives	UWS Shared Drives UWS OneDrive Encrypted USB Drive My Documents Folder on Hard Drive and MAC Equivalent Unlocked desk drawers	Locked drawers, cabinets, safe UWS shared drives (may be restricted to small user group). UWS OneDrive with password protection in place.	Locked drawer, cabinets, safe where access is strictly limited to those with permission to access UWS Vault UWS Shared Drive where access is strictly limited to individuals permitted access

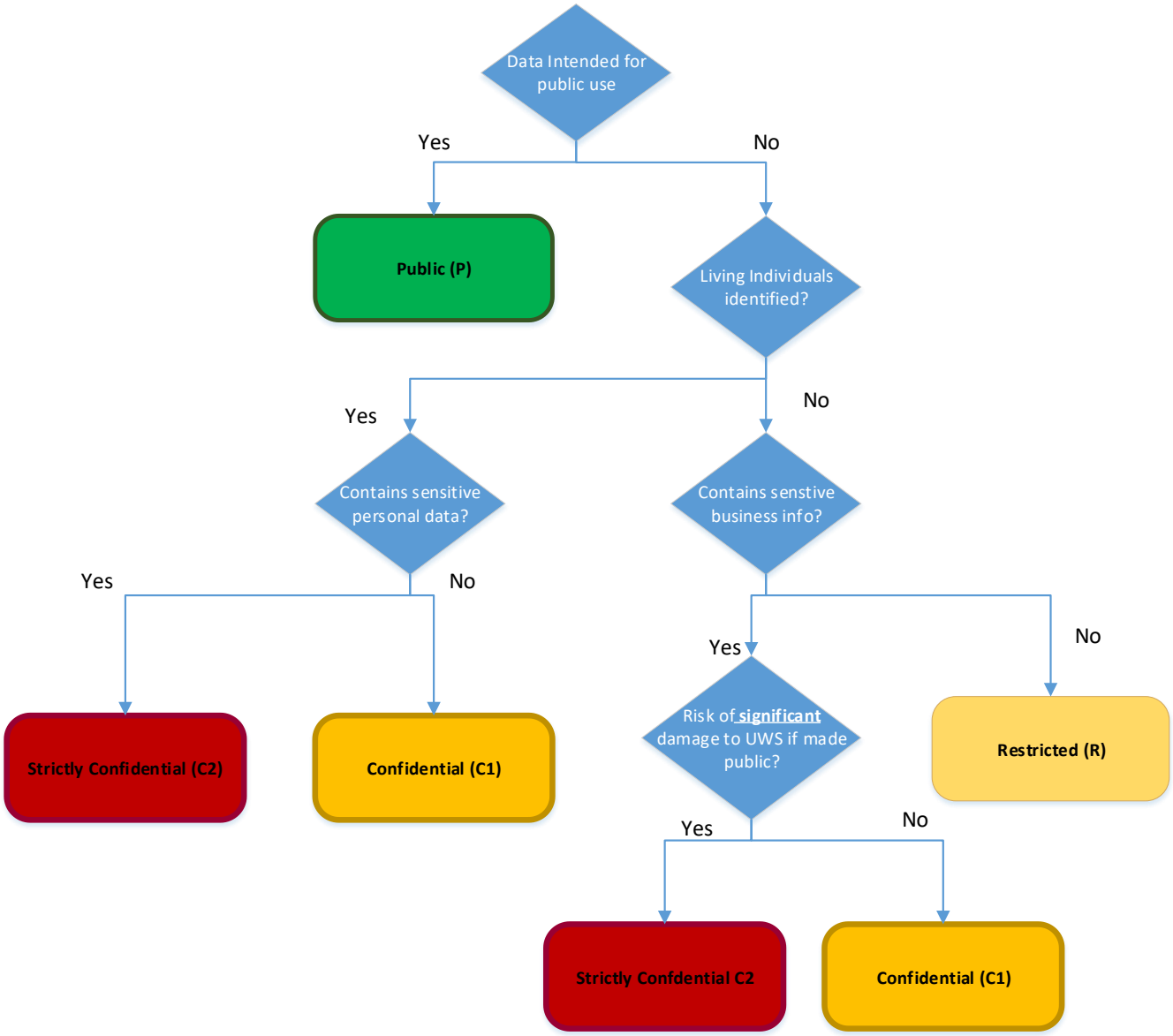
	My Documents Folder on Hard Drive and MAC Equivalent Unlocked desk drawers. On shelves and open spaces		3rd party external service providers storing or processing UWS data where DPIA† completed. Specific secured application intended to store data – e.g. Student transcripts - Banner	
Cannot be stored in/Requires Permission	UWS Vault**	Personal cloud storage - DropBox/Google Drive etc. Non-Encrypted USB Drives UWS Vault	Personal cloud storage - DropBox/Google Drive etc. USB Drives/Local device storage My Documents Folder/PC Hard Drive UWS Vault	Personal cloud storage - DropBox/Google Drive etc. USB Drives My Documents Folder/PC Hard Drive

***** Password Protection – Files which are password protected should be documented and the password shared with your line manager. This is to ensure there is no single point of failure with regard to accessing important files. Use of a password vault/safe should be considered where written copies of passwords can be securely locked away and access is strictly limited to those permitted to access the files.

****** UWS Vault is a secure onsite storage option which is accessible via UWS Connect. This is onsite storage space and is strictly limited to 50mb per user. As such it should only be used to store data in the 'Strictly Confidential C2' category. Files in this area can be shared with colleagues in the same way OneDrive files are shared. Data owners must ensure any data shared is done so responsibly and that any recipients have legitimate reasons for access.

† DPIA – Data Privacy Impact Assessment contact legal@uws.ac.uk

Data Classification Flowchart



This chart can be used to help determine which data classification should be applied to files and documents.

It may be that data may have different classification throughout its lifecycle. For Example, prior to use exam papers should be classed as 'Confidential'. Once used they can be classified as 'Restricted'

Where a range of data is contained e,g. in a database, the highest identified classification should be applied to the full information set