UNIVERSITY OF THE WEST of SCOTLAND

UWS

Data Handling and Classification Protocol

Version – v1 – April 2024

Procedure Author – Head of Legal Services and IT Security and Customer Support Manager

Procedure Owner – Director of Information Services

Parent Policy Statement – Information Services

Public Access or Staff Only Access – Public

Version – v1 April 2024

Changes and Reason for Changes – New Protocol

DOCTRINA PROSPERITAS

Data Handling and Classification Protocol

1. Purpose & Scope

The University creates and holds a wide variety of data and it is important that we have processes and measures in place to protect this data against unauthorised access, disclosure or misuse.

This protocol puts in place a framework that staff should follow for classifying, handling and storing the data we hold to ensure appropriate degrees of protection are applied consistently across the University to prevent personal data and security breaches and minimise the impact of any breaches that do occur.

It is one of a range of measures we have in place to ensure we meet our information security obligations under the UK General Data Protection Regulation and Data Protection Act 2018

This protocol applies to all staff and partners of the University including agency staff, data processors, third parties and any other external collaborators. This protocol also applies to any enrolled post-graduate research students of the University.

This protocol covers all data or information held by the University, in any format. This includes paper notes, documents, electronic files, video and audio recordings. It is particularly important to take appropriate security measures in relation to personal data but this protocol also applies to non-personal data, such as commercially sensitive University information.

2. Classification of Data

The categories are based on the level of sensitivity of the data and the impact on the University should that data be disclosed, accessed, lost or destroyed without authorisation.

All data owned, used, created or maintained within the University should be categorised into one of the following four categories: Public (P), Internal (I) Restricted (R) and Confidential(C).The table set out in the Appendix A explains the types of information which falls within each of these categories, who should have access to this information, how and where the information should be stored or transferred securely and the methods of disposal that should be used.

3. Responsibilities

The Director of Information Services is responsible for approving this protocol and for promoting and publicising the classification protocol and the importance of its use.

All University data, regardless of the format, must be assigned a data owner. This will normally be the author of the document or the manager/head of department of the area responsible for creating the data.
As a data owner you are required to:

- Ensure the appropriate classification is assigned to the data you are creating to assist with appropriate data handling,
- Manage appropriate access to the data,

- Identify additional controls required to ensure the confidentiality, integrity and availability of the data as set out in the data classification schedule,
- Communicate the handling requirements to other users of the data, and
- Ensure data is disposed of in a suitable way when you no longer need it in line with the University records retention schedules.

Data Classification

It is acknowledged that it will not be possible to mark every single document in the University with a data classification, however, it is the responsibility of all staff to have awareness of the four data classifications and the way data within each category should be handled, regardless of whether the data is formally marked or not. For the majority of information it is likely to be obvious which category it falls 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.

Appendix B provides guidance about how you can use M365 to classify documents.

The classification of a document may change over time. For example, a confidential document may move to a lower classification over time if the commercial sensitivity reduces over time.

All staff, whether or not they are the data owner, are responsible for handling University data in line with this protocol and for making sure appropriate protection is in place. Staff working with partners and third parties are responsible for bringing this protocol to their attention.

4. Data Protection

The Data Protection Act 2018 and UK General Data Protection Regulation set out the obligations that apply to the University when handling Personal Data. The University has a Data Protection Code of Practice which sets out how we meet our responsibilities under the legislation and staff should make sure they are aware of the content of the Code of Practice. Importantly, the Code of Practice provides information about how staff should report a data breach if they become aware of one.

5. Further Information

If there are any questions about this protocol you should contact the Legal Services team at legal@uws.ac.uk

Appendix A

	Classification			
	Public	**Internal**	**Restricted**	**Confidential**
Personal Data	Contains no personal data or Personal Data that would be reasonably expected by the individual to be public.	Contains Personal Data that the individual would not normally expect to be made public but is normally available to all University staff or a specific group of University staff	Contains Personal Data where disclosure would not normally be expected by the individual except to a specific group of University staff using appropriate controls and unauthorised disclosure would cause some damage and distress.	Contains 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 Data about an individuals criminal convictions or alleged offences
Examples	Personal Data made public on university websites or social media with the consent of the individual	On-line directory of staff contact details.	• HR records; • Student records such as academic transcripts and attendance details; • Databases and spreadsheets containing personal data of staff or students; • Personal data within email messages	• Occupational Health records. • Email messages containing special categories of personal data (that is not in an anonymised form). • Disciplinary proceedings;

Other Data	Data of no commercial value or sensitivity.	Data of limited commercial value or sensitivity.	Data of serious commercial value or sensitivity.	Data of critical commercial value or sensitivity.
Examples	• Freedom of Information responses; • Information within the Publication Scheme (including Policy Statements & Procedures); and, • Information published on the University website, such as course information or press releases	• Committee minutes and papers marked as open • Departmental Intranet content. • Teaching materials. • Procedures or protocols that are not published on the University website.	• Commercial Contracts; • Closed committee minutes and papers; • Financial information (not disclosed in Financial Statements); and, • Research proposals	• Certain commercial contracts containing market sensitive information. • Internal reports and papers containing market sensitive information • Legally privileged information, such as advice from external legal advisors. • Research papers intended to lead to patentable results (If research is ongoing and has not been published)

Data Storage	Can be stored on any University approved storage location. No restrictions on printing and copying this data, subject to copyright restrictions. Suitable storage locations include MS Teams, OneDrive or publication on the University website or staff intranet.	Can be stored on most University approved storage location that are not public. Data must be held within OneDrive or MS teams where access is limited to University employees. Paper documents must be kept in a desk drawer	Data must be held within systems provided or sanctioned by the University for individual departments. For example, Banner for student data or on OneDrive with appropriate categorisation. Data must not be moved from these locations without appropriate approval. Paper records should not be left unattended and should be stored in locked drawers or cabinets.	Data must be held within systems provided or sanctioned by the University for individual departments, for example where Banner is provided for student data and data must not be moved from that location without appropriate approval. Data can be stored on OneDrive or any cloud based system where this has been authorised by IT and appropriate training completed. Paper records should not be left unattended and must be stored in locked drawers or cabinets.

Data Access	No restriction	Appropriate controls should limit access to only those members of the University that require it.	Data should only be placed in areas with restricted access. Data held within University sanctioned systems must have relevant access controls to appropriately trained staff only with access rights being regularly reviewed. Staff should be aware that OneDrive is linked to an individual user so as part of the leavers process managers are required to ensure files are appropriately transferred to another staff member with the assistance of IT.	Data should only be placed in areas with restricted access. Data held within University sanctioned systems must have relevant access controls to appropriately trained staff only with access rights being regularly reviewed. Staff should be aware that OneDrive is linked to an individual user so as part of the leavers process managers are required to ensure files are appropriately transferred to another staff member with the assistance of IT.
Data Transfer/Sharing	Data may be freely transmitted without restriction.	Data sent via internal email with appropriate care in addressing. Links to OneDrive location of data can be used. Data should not be transferred to any non-UWS approved devices.	Data within information systems should be accessed within that system and not otherwise exported or shared, without data owner approval. If transfer or sharing is required, then appropriate controls must be used to safeguard the data taking in to account the nature and volume of the data being exchanged and the impact of inappropriate disclosure. Encryption must be used when emailing data to external recipients unless	Data within information systems should be access within that system and not otherwise exported or shared without data owner approval. If transfer or sharing is required then appropriate technology, such as encryption, must be used to safeguard the data. Hard copies of documents should be hand delivered internally. External mail should be special delivery signed for and double enveloped.

			approved by data owner. Items sent by internal and external mail should be placed in sealed envelopes. USB storage devices should not be used unless pre-approved by IT and the drive must be encrypted.	USB storage devices should not be used unless pre-approved by IT and the drive must be encrypted.
Disposal	No restrictions but disposal should be in line with the University records retention schedules	Shredding not routinely required. Electronic media must be securely wiped. Disposal should be in line with the University records retention schedules.	Paper document must be shredded. Electronic media must be securely wiped. Disposal should be in line with the University records retention schedules.	Paper document must be shredded. Electronic media must be securely wiped. Disposal should be in line with the University records retention schedules.

Appendix B
Data Classification

Currently, all documents created within M365 are allocated a categorization of 'Internal'. This can be changed by selecting the arrows shown below. Categories should be appropriately assigned as outlined in the Data Classification Schedule. You will be asked to specify a reason for the categorisation change. Select the most appropriate.