Guidance on Use of USB Storage Devices

Version 4 – February 2025

Procedure Author – IT Security and Customer Support Manager

Protocol Owner – Vice Principal (Finance and Infrastructure)

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version v4 –February 2025

Changes and Reason for Changes – Minor updates and formatting changes

GUIDANCE ON USE OF USB STORAGE DEVICES

Using USB devices poses a risk to the University as their use can result in data being lost, stolen or cyber threats being introduced to UWS systems. If data is lost it may result in reputational damage for the University through loss of research and/or potential fines under current data protection legislation. USB storage devices should not be used for storing or backing up data without prior agreement with IT and (depending on category of date) the UWS Legal Services Team. When saving data to any location the Data Handling and Classification Protocol must be followed. Data sharing agreements which require Legal Services agreement should be in place for any external partners\suppliers.

Currently a procedure is in place requiring all USB storage devices to be encrypted prior to use. Exemptions can be made on request to the IT department via a change request.

Where possible USB storage devices should not be used.

Below are some of the risks associated with USB storage usage and recommended alternatives for data storage, backup and sharing.

Risks:

- USB drives can easily be lost or stolen which can result in compromise of sensitive or personal data.
- They can fail, suffer corruption, or be damaged resulting in loss of data.
- Can enable the spread of cyber threats as they tend to get used on multiple devices.
- Are often used as a backup of data stored in other locations resulting in duplicate data which can quickly become out of date, impacting on data integrity
- Puts you at greater risk of being responsible for accidental data loss/data leakage.

Guidance

- Microsoft OneDrive and Teams provide a secure storage area. Any data categorised as 'Confidential' or 'Sensitive' should be stored within a secure Teams environment. If you require a 'Secure Team created, contact the IT Service Desk.
- 'Confidential' or 'Sensitive' data should never be held on a USB drive.
- OneDrive and Teams files can be shared with colleagues and third parties where appropriate. Adding external collaborators to Teams groups can be requested via the IT Service Portal using a 'Change Request'
- Files stored on OneDrive/Teams should follow the requirements of the UWS Data Handling and Classification Protocol. When a staff member leaves the University, any data stored on their OneDrive or Teams will only be available for 90 days after their leaving date.
- Other cloud storage locations including but not restricted to DropBox and Google Drive must not be used to store UWS data storage without prior agreement from IT or Legal Services. Misuse of University data may result in fines and/or disciplinary action. If you wish any further information regarding secure file storage, please contact Information Services.

Further Information:

Further information regarding the University's requirements and legal commitments can be found within the following documents available on the following page of the University's website https://www.uws.ac.uk/about-uws/policies-procedures-guidance/

Related Documents:

- IT Information Security Procedure
- Data Handling and Classification Protocol
- UWS Data Protection Code of Practice