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 malware 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 the data protection legislation. 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
- External hard drives and USB drives can fail, resulting in loss of data.
- USB devices are often the source of and reason for the spread of malware as they tend to get used on multiple devices.
- USB devices are often used as a backup to network storage options. This results in duplicate data which can quickly become out of date which may lead to a data protection breach.
- Saving to portable devices puts you at greater risk of being responsible for accidental data loss/data leakage.

Safer Alternatives:

- Your departmental shared drive (normally G:\). This storage is held within the university, is secure and can be accessed by you externally using VPN. This drive should be used for any data which can be safely shared with colleagues.
- The Vault (available via https://connect.uws.ac.uk/) highly confidential data such as Special Category student information, data which may be sensitive to the organisation.
- Microsoft OneDrive Business account/ MS Teams. As a staff member you have 1 Terabyte of storage in the Microsoft Cloud. This provides secure storage for all but the most sensitive of documents and should be used for day to day working documents. OneDrive files can be accessed off campus from personal devices such as laptops, phones and tablets. OneDrive and MS Teams files can also be shared with colleagues and 3rd parties if appropriate. Files saved to OneDrive / MS Teams can be moved to your UWS shared drive but must never be moved to the hard drive of a personal device. Files saved to OneDrive should follow the requirements of the UWS Data Classification Schedule. When a staff member leaves the University their data stored on OneDrive will no longer be available 90 days after their leave 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 helpdesk@uws.ac.uk or Legal Services legal@uws.ac.uk

If you have no option other than to use a USB storage drive, ensure it is encrypted using Bitlocker:

- Connect the Drive to your PC
- Open Windows Explorer
- Find the removable drive from the list and click with the right mouse button
- Select Turn on ‘Bitlocker’

- Create a password to protect the drive (you will use this to access the drive going forward).

Remember, misuse of data or other University resource 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/

- Information Security Procedure
- Cloud Guidelines
- Data Classification Schedule

Procedure Author – IT Security and Customer Support Manager

Protocol Owner – Director of Information Services

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version 3 – March 2023

Changes and Reason for Changes – Minor updates including reference to MS Teams and formatting changes