GUIDELINES ON USE OF USB STORAGE DEVICES

Using USB devices poses a risk to the university because their use can result in data being lost or viruses being introduced to our systems. If data is lost it can result in reputational damage for the University and also 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.

1. **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 facilitate the spread of viruses 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 This results in duplicate data which can quickly become out of date which may lead to a data protection breach.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.

2. **Safer Alternatives:**

- Your departmental shared drive (normally G:\). This storage is held within the university, is secure and can be accessed by you externally via VPN access. This drive should be used for any confidential data such as student details, research data or any other intellectual property or data sensitive to the organisation
- Microsoft OneDrive Business account. 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. One Drive files can be accessed off campus from personal devices such as laptops, phones and tablets. Files can also be shared with colleagues and 3rd parties if appropriate. Files saved to OneDrive can be moved to your UWS shared drive but must never be moved to the hard drive of a personal device.
- DropBox and Google Drive can be used for your own personal files but should not be used for UWS data 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).
- Pre-encrypted drives are available – Contact the IT team for further advice.

If you wish any further information regarding secure file storage, please feel free to contact us.

3. Further Information:

Further information regarding the University's requirements and legal commitments can be found here:

- Information Security Procedure
- Cloud Guidelines
- Data Classification Schedule

Procedure Author – Information Security Manager	Procedure Owner – Director of IT
Parent Policy Statement - IT Policy Statement	Public Access or Staff Only Access - Public
Version 1 – 1st July 2019	Changes and Reason for Changes – New Guidelines