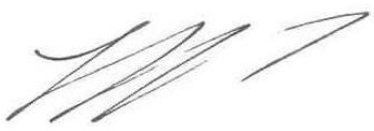
Sheffield Hallam University

Bring Your Own Device (BYOD) Policy for University Staff

Issuing Authority:	Simon Briggs, Director of Digital Technology Services
Signed:	
Effective Date:	February 2023
Version:	2023.2

Bring Your Own Device (BYOD) Policy for University Staff

Objective

This policy defines appropriate use by University staff whilst using *their own* devices for accessing, viewing, modifying and deleting of University held data and accessing its systems.

Scope

This policy applies to all University staff and other authorised non-student users who have access to the University IT services and data, hereafter referred to as "staff".

This policy covers the use of personally owned electronic devices to access and store University information. Such devices include smartphones, tablets, laptops, desktop computers and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

Policy Requirements

The University wishes to support staff in the use of technology but needs to balance this with both requirements for compliance with security standards such as Cyber Essentials, and its legal duties as a Data Controller in order to protect the information it holds relating to staff, students, partners and others.

We recommend that:

- *Wherever possible* you access University data and services from a University managed device.

- If this is not possible then you should only access University data and services from a BYOD device using a University provided web service. These include:
    - Remote File Access service
    - Outlook Web Access and Office 365 on the web
    - Remote Desktop

- University data should only be downloaded to your personal devices if *neither of the 2 above options is available to you*.

If you are in any doubt as to whether particular data can be stored on your device you are required to err on the side of caution and consult with your manager, or seek advice from the ***IT Service desk*** or from the ***University Information Governance Officer***

Please note that the University must reserve the right to refuse, prevent or withdraw access to users and/or devices or software where it considers that there are unacceptable security or other risks, to its staff, students, business, reputation, services or infrastructure.

System, Device and Information Security

The University takes information and systems security very seriously and invests significant resources to protect data and information in its care. If you use your own device as a work tool you are expected to take some basic steps to maintain the security of the University information that you access.

In practice, this means:

- Use device security features, such as a PIN, Password/Passphrase and automatic lock to help

protect the device when not in use. Passwords should comply with the University Password Policy. If you set a PIN for a mobile device it must be at least 6 digits long and you should use different PINs for any devices where you have used them.

- Use encryption to protect data on the device. The University encryption policy can be found **here** and guidance on how to use encryption is available **here**.
- Keep the device operating system and software up to date, for example usinf Windows Update or Software Update services. Where possible enable Automatic Updates so that important updates will be automatically installed.
- Install and configure tracking and/or wiping services, such as Apple's 'Find My', Android's 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.
- Install and use anti-virus software on Windows and Macintosh computers. This can be tools built into Windows or Mac OS or alternative tools users might prefer.
- Do not attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' or 'Root' the device if it is being used to access University IT services.
- Only use accounts with administrative or root privileges when necessary and do not use them for day-to-day tasks such as web browsing or reading email. The impact of malicious software can be many times greater if it is run by privileged accounts.
- Regularly check the user accounts present on devices that use them such as Windows or Mac computers and remove any that are no longer required.

All of these steps will help ensure that *your own personal data is also protected*.

Additional important steps include:

- Remove any University information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets, as soon as you have finished using them.
- Limit the number of emails and other information that you are synchronizing to your device to the minimum required.
- Remove all University information from your device and return it to the manufacturers' settings before you sell, exchange, or dispose of your device. See **here** for advice and guidance.

In the event that your personal device is lost or stolen or its security is compromised, you should promptly report this to the ***IT Service desk*** in order that they can assist you to change the password to all University services (it is also recommended that you do this for any other services that have accessed via that device, e.g. social networking sites, online banks, online shops).

You may also be asked to cooperate with University officers in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.
Further advice on securing personal devices is available from the **IT Help Webpages**

Monitoring of User-Owned Devices

The University will not monitor the content of your personal devices, however the University reserves the right to monitor and log data traffic transferred between your device and University systems, both over internal networks and entering the University via the Internet.

In very exceptional circumstances, for instance where the only copy of a University document resides on a personal device, or where the University requires access in order to comply with its legal obligations (e.g. under the Data Protection Act 1998, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) the University will seek your support in resolving an issue with University information stored on your personal device.

If online access is not feasible and you legitimately need to access or store sensitive information, such as student or financial records on your own device for a limited period, you must seek authority from your Line Manager. The University may then need to monitor the device at a level that may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data.

Support

The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage, resulting from support and advice provided.

Use of Personal Cloud Services

Personal data as defined by the General Data Protection Regulation and University confidential information may not be stored on *personal* cloud services[1] in line with the **University Cloud Storage Policy.**

Compliance Sanctions and Disciplinary Matters

Any breach of this policy may result in action being taken under the Problem Resolution Framework for **staff**

Other Supporting Documents

Regulations for the Use of IT Facilities and Learning Resources **Electronic Data Encryption Policy**

Cloud Storage Policy Overview

Staff Responsibility for Information Security

Staff Who Work Off-Campus or With Their Own Equipment

Advice and Guidance

Advice and guidance is available via IT Help:

Web: **Using Your Own Computer or Device**

IT Service Desk: ***IT Service desk***

Advice and guidance on Data Protection legislation are available from the University's Data Protection Officer or the **Data Protection Webpages**

[1] *Such as Apple iCloud, Dropbox, Google Drive, Microsoft OneDrive, etc.*