Using Your Own Device Policy

1. Purpose and Context

This document describes acceptable use pertaining to staff whilst using their personally owned computing devices to access University Computing Systems and Services and the storing of confidential data on those devices.

2. Scope

These regulations apply to any member of staff using their own device for University purposes. A computing device is any digital equipment that can access University systems and data, including desktop computers, laptops, tablets, and smartphones. University systems are any on-campus or cloud-based platforms that store or process University information including, but not limited to: Office 365 email and calendar, SharePoint, Microsoft Teams, UniDesktop, the "Remote" service offered by Azure Virtual Desktop (AVD), and Global Protect VPN.

3. Introduction

The University recognises the benefits that can be achieved by allowing staff to use their own devices whilst working, whether this is at home, on campus or whilst travelling.

This policy is however, about reducing the risk when using your own device, risks include devices being lost or stolen; being used by others who are not authorised to access University information or being exploited in such a way to put University data at risk.

4. Information Security Policies

All relevant University policies still apply to staff using their own devices. Staff should be familiar with the University's Information Security related policies which are directly relevant to staff using their personal devices.

- IT Security Procedure Manual
- IT Security Policy
- Data Protection Policy
- Computing Regulations
- Code of Practice for Research

5. Responsibilities of Staff Members

Staff using their own devices must:

- Avoid storing sensitive or confidential University information on personally owned devices. Where sensitive or confidential information must be accessed, an approved access solution such as UniDesktop, the "remote" service (AVD), or remote access to an office computer should be used as data then remains within University systems.

- Where the need to store sensitive and confidential University information locally on a personally owned device is unavoidable, staff must ensure that appropriate encryption is in place.
    - The folder or entire drive in which the data resides must be encrypted using an appropriate strength encryption (see IT Security Procedure Manual section 4).
    - The device itself must be protected by a username and password or PIN that is known only to authorised individuals (see IT Security Procedure Manual section 3.1 for password guidance and 4.4 for PIN guidance).
    - All sensitive and confidential data must be deleted from the device as soon as it is no longer needed, even where the data is encrypted.
- **Not use OneDrive client on personally owned devices to access University accounts** as this systematically synchronises all University data to that device.
    - Instead, documents residing in OneDrive should be accessed via a browser.
- Ensure **anti-virus software** is installed, enabled and automatically updated.
- Ensure **local firewall** is enabled on desktop and laptop computers.
- Ensure that the device hardware is **supported** by its vendor and that **security patches** (often called firmware) are installed within appropriate timescales (see IT Security Procedure Manual section 6.10).
- Ensure operating system software is **supported** by its vendor and that **patches** are installed as soon after release as possible – and always **within 14-days**.
- Ensure application software is **supported** by its vendor and that **patches** are installed as soon after release as possible – and always within the timescales set-out in the IT Security Procedure Manual section 6.10.
- Not circumvent any built-in **mobile device security** systems (known as 'jailbreaking' or 'rooting') in order to download apps from sources other than the official app stores, or to obtain 'super-user' privileges over the device.
- Set up **passwords**, **PINs**, or **biometric** equivalents to access the device. These must be of sufficient length and complexity for the particular type of device (see IT Security Procedure Manual sections 3.1 and 4.4).
- Ensure that others who may use the device **cannot** access University information, for example by using an additional computer account with a separate passcode.
- Set the device to **lock automatically** when the device is inactive for more than a few minutes.
- Avoid **untrusted Wi-Fi network**s such as those in cafes. Disable automatic connection to open, unsecured Wi-Fi networks when using wireless networks outside of the University and make risk-conscious decisions before connecting.
- **Securely delete** all University information from the device when you stop using it (for example because you have replaced it) or when you leave the University's employment.
- Install and configure **tracking and/or wiping services**, such as Apple's 'Find My Iphone/Ipad app', Androids 'Google Find My Device' or Windows 'Find My Phone', where the device has this feature.
- Download applications ('apps') or other software from **reputable sources** only.

- Uninstall University applications as soon as they are no longer required.
- **Report any data breaches** in accordance with the Data Breach Reporting procedure

6. Registering your Device with University Systems:

To comply with the government's cyber-security certification requirements the University must be able to identify the make and operating system version of devices accessing business data, and check if they receive security updates. This includes personally owned devices used for work purposes.

Staff must register any personally owned devices with University systems when requested. This allows the collection of information required to meet cyber security certification requirements, including the names, makes, models, operating system version, and serial numbers of devices being used. The University will not be able to see any personal data. Detailed information is available from Microsoft here: What info can your company see when you register your device? | Microsoft Learn.

If you do not wish to register your personal devices, then you should not use your personal devices for work purposes.

7. Consequences of non-compliance

The loss, theft or misuse of a personally owned device is personally distressing. If you use sensitive data, it can also have serious consequences for others, for example staff and students about whom information is held. In addition, there may be significant legal, financial and reputational consequences for the University, in relation to the General Data Protection Regulations (GDPR). You may also carry personal responsibility which, in serious cases could result in disciplinary action under the IT Security Policy.

8. Where to get help

If you need any assistance with configuring your own device to work with the university's systems as specified above then please visit HudHelp or contact IT via Support IT.Support@hud.ac.uk or telephone Extension 01484 473737. The team should be able to help or can escalate your query to the relevant team if appropriate.

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Using Your Own Device Policy.docx
Version Number:	3.2
Equality Impact Assessment:	January 2019
Approved by:	SLT
Effective from:	30/11/2023
Date for Review:	October 2024
Author:	Information Security Manager
Owner (if different from above):	
Document Location:	https://www.hud.ac.uk/media/policydocuments/Using-Your-Own-Device-Policy.pdf
Compliance Checks:	Breaches of the Regulations handled under the respective staff University disciplinary processes.
Related Policies/Procedures:	IT Security Policy IT Security Procedure Manual Computing Regulations Data Protection Policy

REVISION HISTORY			
Version	**Date**	**Revision description/Summary of changes**	**Author**
V1.0	October 2017	First draft using Policy Framework. Minor drafting updates.	Derek Heathcote
V1.1	January 2019	Added additional links to GDPR and security policy. Added a section on where to get help	Alan Radley
V1.2	June 2020	Minor change to put stronger emphasis on encryption in section 5 "*Encrypt any device*	Alan Radley

		where sensitive or confidential university information is stored Change to include reference to OneDrive 'Sync' and encrypting the folder/drive	
V2.0	September 2021	Changes to align to major update of IT Security Policy. Removal of permission to install OneDrive client on personally owned devices	Information Security Manager
V3.0	October 2022	Changes to scope to clarify device types in scope. Addition of local firewall requirement. Addition of hardware vendor support requirement. Addition of mobile device security systems requirement.	Information Security Manager
V3.1	November 2022	Addition of device registration.	Information Security Manager
V3.2	November 2023	Addition of AVD to Section 2: Scope Addition of requirement to remove University applications when no longer required. Addition of requirement to keep installed applications patched and within vendor support.	Information Security Manager