Using Your Own Device Policy

1. Purpose and Context

This document describes acceptable use pertaining to staff members, affiliates and third-party contractors / service providers whilst using their personally owned computing devices to access University Computing Systems and Services and the storing of confidential data on those devices.

The University recognises the benefits that can be achieved by allowing staff, affiliates, and third-parties to use their own devices whilst working, whether this is at home, on campus, or whilst travelling; this does however introduce additional information and data governance risk.

This policy is about reducing and managing 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.

2. Scope

These regulations apply to any member of staff, affiliate, or other third-party contractor / service provider using their personally owned device to access or store University data. 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. Information Security Policies

All relevant University policies continue to apply to those using their personally owned 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

4. Responsibilities of Staff Members

Staff, affiliates, or other third-party contractors / service providers using their own devices must:

- Not download and store sensitive or confidential University information on personally owned devices. Where sensitive or confidential information must be accessed, an approved solution such as the "remote" service (AVD), UniDesktop for remote access to an office computer, or a University issued laptop should be used as data then remains within the University ecosystem.
- **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.
- Not use Box Drive client (for Research use only) on personally owned devices to access University accounts as this systematically synchronises all University data to that device.
    - Instead, information residing in Box Inc. should only be accessed via a browser.
- Ensure **anti-virus software** is installed, enabled and receives updates automatically.
- 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 profile with a separate password or PIN.
- 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 profiles and 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

5. 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.

The University will implement technical controls that prevent access to University systems and data from personally owned computing devices that fail to meet the criteria for vendor supported operating systems and other requirements as outlined in Section 5 of this policy.

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.

6. Using Personal Devices on Campus

Staff are permitted to connect personal mobile devices such as laptops, tablets, and smartphones to the University's eduroam and WiFi-Guest wireless provisions but must not connect any personal device to the wired campus network. Only University maintained computer devices are permitted to connect to the wired campus network.

7. Consequences of non-compliance

The loss, theft or misuse of a personally owned device is personally distressing. If you have downloaded or stored sensitive or confidential data, then the loss or theft of that device 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

The University's IT Security Procedure Manual Section 4.3 offers guidance on using your own device including how to check if your operating system is supported by its vendor.

If you need any assistance then please visit HudHelp or contact IT Support via IT.Support@hud.ac.uk or telephone Extension 01484 473737.

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Using Your Own Device Policy.docx
Version Number:	4.0
Equality Impact Assessment:	January 2019
Approved by:	SLT, 11/02/2026
Effective from:	30/11/2025
Date for Review:	November 2026
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
V3.3	November 2024	Addition to Section 6 relating to technical controls to restrict access from out of support operating systems. Insertion of new Section 7 relating to use of own devices on campus networks.	Information Security Manager

		Renumbering because of the insertion of new Section 7. Addition to Section 9 signposting staff to more guidance in the IT Security procedure Manual.	
V4.0	November 2025	Combined a previous Introduction section into the Purpose and Context section. Clarified the scope of usage to staff members, affiliates and any other third-party contractors / service providers through the document. Updated Responsibilities to mandate that sensitive and confidential information must not be saved to personally owned devices (section 4). Replicate the OneDrive client control for Box Drive client.	Information Security Manager