

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.

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; these 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 information on personally owned devices. .
Where sensitive or confidential information must be accessed, an approved access solution, such as via UniDesktop or remote access via VPN 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 that is known only to authorised individuals.
- 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 operating system software is supported by its vendor and that security patches are installed as soon after release as possible – and always within 14-days.
- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device (see IT Security Procedure Manual section 3.1).
- 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 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 'Where My Droid' or Windows 'Find My Phone', where the device has this feature.
- Download applications ('apps') or other software from reputable sources only.
- Report any data breaches in accordance with the [Data Breach Reporting procedure](#)

6. 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](#).

7. 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 contact IT Support ITSupport@hud.ac.uk or telephone Extension 3737. 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 |
| Version Number: | 2.0 |
| Equality Impact Assessment: | January 2019 |
| Approved by: | Information Governance Group |
| Effective from: | 31 October 2021 |
| Date for Review: | October 2022 |
| 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: | Annual compliance survey (personally owned devices) |
| Related Policies/Procedures: | IT Security Policy Computing Regulations |

REVISION HISTORY

| Version | Date | Revision description/Summary of changes | Author |
|----------------|--------------|---|------------------------------|
| V1.0 | October 2017 | First draft using Policy Framework. Minor drafting updates. | Information Security Manager |
| V1.1 | January 2019 | Added additional links to GDPR and security policy. Added a section on where to get help | Information Security Manager |
| V1.2 | June 2020 | Minor change to put stronger emphasis on encryption in section 5 " <i>Encrypt any device where sensitive or confidential university information is stored</i> Change to include reference to OneDrive 'Sync' and encrypting the folder/drive | Information Security Manager |

| | | | |
|------|----------------|--|------------------------------|
| 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 Update to compliance checks | Information Security Manager |
|------|----------------|--|------------------------------|