University of HUDDERSFIELD
Inspiring tomorrow's professionals

# Using Your Own Device Policy

## 1. Purpose and Context

This document describes acceptable use pertaining to staff whilst using their personally owned 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, stolen 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 note, in particular, 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

Individuals who make use of their personal device for storing work related data e.g. email must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of University information.
- Invoke the relevant security features, such as passwords, tracking and locking services (see below for further detail).
- Maintain the device ensuring it is regularly patched and upgraded.
- Ensure that the device is not used for any purpose that would be at odds with the University of Huddersfield's Computing Regulations.

Computing & Library Services will always endeavour to assist colleagues wherever possible but cannot take responsibility for supporting devices it does not provide. Staff using their own devices must therefore take reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential where appropriate.
- Maintain the integrity of data and information.

**Staff using their own devices must:**

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.
- 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.
- Set the device to lock automatically when the device is inactive for more than a few minutes.
- Keep operating system software up to date.
- Disable automatic connection to open, unsecured Wi-Fi networks when using wireless networks outside of the University, and make risk-conscious decisions before connecting.
- Ensure that others who may use the device cannot access University information, for example by using an additional account passcode.
- 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.
- Download applications ('apps') or other software from reputable sources only.
- Encrypt documents and devices.
- Use anti-virus software and keep it up to date.
- Avoid storing sensitive or confidential information on personally owned devices. Instead, use Unidesktop to access information on University systems, or a University-approved secure cloud storage service.
- Delete information belonging to the University as soon as possible once it is no longer required. This includes information contained within emails.
- Report any data breaches in accordance with the IT Security Procedure Manual.

## 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. You may also carry personal responsibility which, in serious cases could result in disciplinary action under the IT Security Policy.

| POLICY SIGN-OFF AND OWNERSHIP DETAILS | |
|---|---|
| **Document name:** | Using Your Own Device Policy |
| **Version Number** | 1.0 |
| **Equality Impact Assessment:** | October 2017 |
| **Approved by:** | IGG 23/11/2017 |
| **Effective from:** | 23/11/2017 |
| **Date for Review:** | December 2018 (as part of IT Security Policy) |
| **Author:** | Derek Heathcote |
| **Owner (if different from above):** | Head of Computing Services |
| **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<br>Computing Regulations |

## REVISION HISTORY

| Version | Date | Revision description/Summary of changes | Author |
|---|---|---|---|
| V1.0 | 23/11/2017 | First draft using Policy Framework. Minor drafting updates. | Derek Heathcote |