Using Your Own Device Policy

1. Introduction

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

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.

2. 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

3. 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.

Approved by University Information Governance Group 14/6/2016
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 systems software up to date.
- When using wireless networks outside of the University, control connections by disabling automatic connection to open, unsecured Wi-Fi networks and make risk-conscious decisions before connecting.
- If others use your device, ensure they cannot access University information, for example with an additional account passcode.
- When you stop using your device (for example because you have replaced it) and when you leave the University’s employment, securely delete all University information from your device.
- Only download applications (‘apps’) or other software from reputable sources.
- Encrypt documents and devices.
- Use anti-virus software and keep it up to date.
- Sensitive or confidential should not be stored on personally owned devices. Instead, use Unidesktop to access information on University systems, or use a University-approved secure cloud storage service.
- Where it is essential that information belonging to the University is held on a personal device it should be deleted 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.

4. **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.