Bring Your Own Device Policy (BYOD)

1. INTRODUCTION

Whilst the University of Northampton (UON) expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment. This policy may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this policy may be addressed via the University's Disciplinary Policy and Procedure, and Code of Conduct Policy.

This policy will be reviewed by the IT Services and Human Resources departments on a 3-year basis or amended in response to changes in future legislation and/or case law.

2. OWNERSHIPS

The IT Services and Human Resources departments owns and manages this policy on behalf of the University.

3. ORGANISATIONAL SCOPE

This is a University policy that applies to all employees, students, and contractors of the UON, and any applicable 3rd parties working on behalf of the UON. This also includes any wholly owned subsidiaries, unless an alternative applicable policy exists, for example PCI-DSS. The Finance department is not eligible to use their own devices due to the University's PCI-DSS compliance commitments. Those in scope will be referred to as 'Users' for the purpose of this document.

4. POLICY STATEMENT

The purpose of this policy is to provide a consistent and secure approach to mitigating the risks of the use of personal devices to access UON IT Resources, both on and off premises. BYOD raises a number of data protection concerns because the device is owned and managed by the User rather than the University.

If Users have been supplied a University owned mobile device by the UON, the preference should be to use this as the default device for work purposes rather than personal equipment. If a User wishes to use a BYOD device to access UON IT Resources and data, they may do so if they follow the requirements of this policy and the advice and guidance provided through the IT Service Desk.

It is UON’s intention to place as few technical and policy restrictions as possible on BYOD, subject to the University meeting its legal, regulatory, and duty of care obligations.

5. DEFINITIONS

Anti-virus
Software designed to detect and remove viruses from a computer/device.

BYOD
The practice of allowing employees of an organisation to use their own computers, smart phones, tablets, or other electronic devices for work purposes.

Data
Includes but is not limited to any information accessed, stored, and/or processed on/by IT Resources, stored either digitally or hardcopy, in formats including, but not limited to: text, graphics, images, sound, and video.

Encryption
Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the internet.

End of Life
A device that does not receive support or it is at the end of its useful life.

IT Resources
All assets that connects to the UON network, and/or contains, accesses, stores, and/or processes UON data. This includes, but is not limited to: desktop computers, laptops, smartphones, tablets, servers, printers, data and voice networks, networked devices, software, applications, electronically-stored data, portable data

storage devices, hardcopies, third party networking services, telephone handsets, and video conferencing systems.

OneDrive
OneDrive is Microsoft's service for hosting files in the 'cloud'. OneDrive is a simple way to store, sync and share files.

Sensitive Data
There are three main types of sensitive data, including but not limited to: **personal** (this is data from which an individual/individuals are personally identifiable. It includes names, contact details (phone, address, email), initials, financial information. It can include any identifier of an individual, e.g. a job title can be personal data if it alongside other information that would allow someone to identify the individual), **special category** (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, biometric data, or data concerning health, a person's sex life, or a person's sexual orientation) and **confidential** (information which is confidential to the University for example for business reasons. This can include meeting papers and minutes, proposals for discussion, research and intellectual property, financial information like individual bank details or details of contracts. If you are unsure about the confidentiality of data, check with your line manager or the person/team which originated the data). This data must be protected from unauthorised access to safeguard its privacy and the security of individuals and the organisation.

USB
A small electronic device containing memory, that is used for storing data or transferring it to or from a computer, digital camera, etc.

6. KEY PRINCIPLES

6.1. Access

- Devices over 5 years old with legacy firmware or software, may not be compatible with the University Wi-Fi.
- By default, any University of Northampton data accessed via a personal device should not be downloaded to that device, except where management approval has been sought and approved in advance. Downloading data to users' University OneDrive account is permitted but not to users' personal OneDrive

account, or any other document sharing or collaboration site that is not managed by the University of Northampton.

- Any personal devices used to access the UON's systems should be secure, in line with the associated University's security policies and users must comply accordingly.
- Specifically, the following should be applied:
  - Set and use passwords or pin codes on the device (or use of equivalent biometric facilities to personalise log ins). Whenever possible, use a strong password and do not share with password with anyone. (See Acceptable use policy)
  - Users must ensure that their devices are up to date with regular security updates performed.
  - If the operating system is no longer supported the device should not be used. For example, Windows 7, IOS 10 and Android 9 should not be used.
  - Use anti-virus software and keep it up to date.
  - Hard disk and mobile phone encryption should be enabled where possible.
  - Users should take care to ensure their device is securely wiped or disposed of at the end of device's life.
  - Before a device is passed to a new owner any University data should be removed, and any applications removed.
  - The device should not be shared with family members, friends or third parties.
  - To access your University email on a mobile device you should use the Outlook app. This will enable a feature that allows a 'remote wipe' of only University data.
  - Ensure your device locks automatically when inactive.
  - Users should not access UON IT systems or process UON data whilst connected to public Wi-Fi hotspots, where the security measures are unconfirmed, they are almost certainly insecure if 'open'.
  - Do not Root or Jailbreak the device.
  - Only download applications or other software from reputable source.

6.2. Transmission

- Any transmission of UON data to and from the device should be encrypted and authorised. Portable storage media such as USB memory sticks or external hard drives should not be used to store or transfer University of Northampton's data unless the data is classified as PUBLIC i.e. data that is already in the public domain or data that is deemed as of very low sensitivity.

6.3. Sensitive Data

- The University, in line with guidance from the Information Commissioner's Office on BYOD, recognises that there are inherent risks in using personal devices to hold sensitive data. Therefore, the University's policy is that staff must not store or process sensitive data on personal devices.

6.4. Display Screen Equipment (DSE)

- The University advises against prolonged use of portable devices (such as a mobile phone or tablet) and avoid, where reasonably practicable, the use of computer equipment which involve a risk of injury. The University DSE policy should be reviewed for further detail.

7. PROCEDURE

7.1. Updating device and applications

The following link is based on expert advice from the National Cyber Security Centre, giving you up to date, step by step details for how you can update your device and keep your information safe.
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

7.2. Incident Reporting

The loss, theft, or misuse of a BYOD device that contains UON data or applications should be reported to IT Services immediately via the IT Service Desk on 01604 893 333 (Ext. 3333), at the Learning Hub, or using the Service Desk Portal (https://uon.saasiteu.com/Modules/SelfService/#home).

8. ASSOCIATED DOCUMENTS

Acceptable Use Policy
Display Screen Equipment (DSE) Policy
GDPR Policy
Information Security Policy

9. EQUALITY IMPACT ASSESSMENT

There is no adverse equality impact within this policy. All responses to breaches of rights will be dealt with in accordance with this Policy, Procedure and relevant Appendices irrespective of an individual's specific characteristics.

10. VERSION CONTROL

Version Control	1.1	**Approval record**	
Author:	IT Services	Approval:	TU Liaison – 18/09/2018 UMT – 09/10/2018 Boar – 11/12/2018
Date written:		August 2018	
Current status:		Live	
Record of Amendments			

Date	Version number	Details of Change	Approval
11/12/2018	1.0	Policy Created	
04/03/2024	1.1	General Review	ITSB – 24/01/2024