Bring Your Own Device Policy (BYOD)

1 INTRODUCTION

Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and 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.

This policy will be reviewed by the IT Services and Human Resources department 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 department owns and manages this policy on behalf of The University of Northampton.

3 ORGANISATIONAL SCOPE

This BYOD policy is a corporate policy and applies to all employees (and workers, as applicable) and students of The University of Northampton including any wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions, for example PCI DSS.
The Finance department is not eligible to use their own devices due to the Universities PCI-DSS compliance commitments.

4 POLICY STATEMENT

The purpose of this policy is to provide a consistent and secure approach for IT Services to mitigate the risk of the use of personal devices to access the University of Northampton's system.

BYOD raises a number of data protection concerns because the device is managed by the user rather than the University.

The underlying feature of BYOD is that the user owns, maintains and supports the device. This means that the data controller will have significantly less control over the device than it would have over a traditional corporately owned and provided device. The security of the data is therefore a primary concern given that the data controller may have a large number and a wide range of devices to consider

If employees have been supplied a portable device by the UoN, the preference should be to use this as the default device for business purposes rather than personal equipment.

If you wish to BYOD to access University systems, data and information you may do so, if you follow the provisions of this policy and the advice and guidance provided through the IT Helpdesk. It is the UoN intention to place as few technical and policy restrictions as possible on BYOD subject to the University meeting its legal and duty of care obligations.

This policy also applies to using personal devices for work purposes off University premises.

If you are using your own device, you have a responsibility to configure it securely. This policy sets out the minimum requirements.

5 DEFINITIONS

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.

Anti-virus

Software designed to detect and remove viruses from a computer.

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

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

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

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

PCI DSS
Payment Card Industry Data Security Standard. A standard to help business process card payments securely and reduce card fraud.

6 KEY PRINCIPLES

6.1 Access

As part of our new campus, a state of the art network has been developed. As a result, devices over 5 years old, may not be compatible with the University Wi-Fi.

By default, any University of Northampton (UoN) 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 One-Drive account is permitted but not to users' personal One-Drive 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 code 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 Password Protocol).
- 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 Vista security updates ended April 11, 2017 and 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 for more than a few minutes.
- 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'.
- Only download applications or other software from reputable source.

6.2 Transmission

Any transmission of data to and from the device should be encrypted. 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 Data Protection

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 personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data.

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.cyberaware.gov.uk/software-updates

7.2 Reporting use of personal device

On joining the University, the HR department notifies IT of new employees. If BYOD is preferable, the employee should inform HR who shall notify the IT department.

If an employee should wish to change to their own device, they should also notify HR.

7.3 Incident Reporting

The loss, theft or misuse of a BYOD 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.

Any loss of a device should be reported to IT Services immediately using the IT Services Portal.

https://itservicedesk.northampton.ac.uk/MSMSelfService/LogAnITIssue.aspx

8 ASSOCIATED DOCUMENTS

- GDPR Policy
- Password Protocol
- Acceptable Use Policy
- Data Back-Up Policy
- Display Screen Equipment (DSE) Policy and procedure

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	1.0	**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