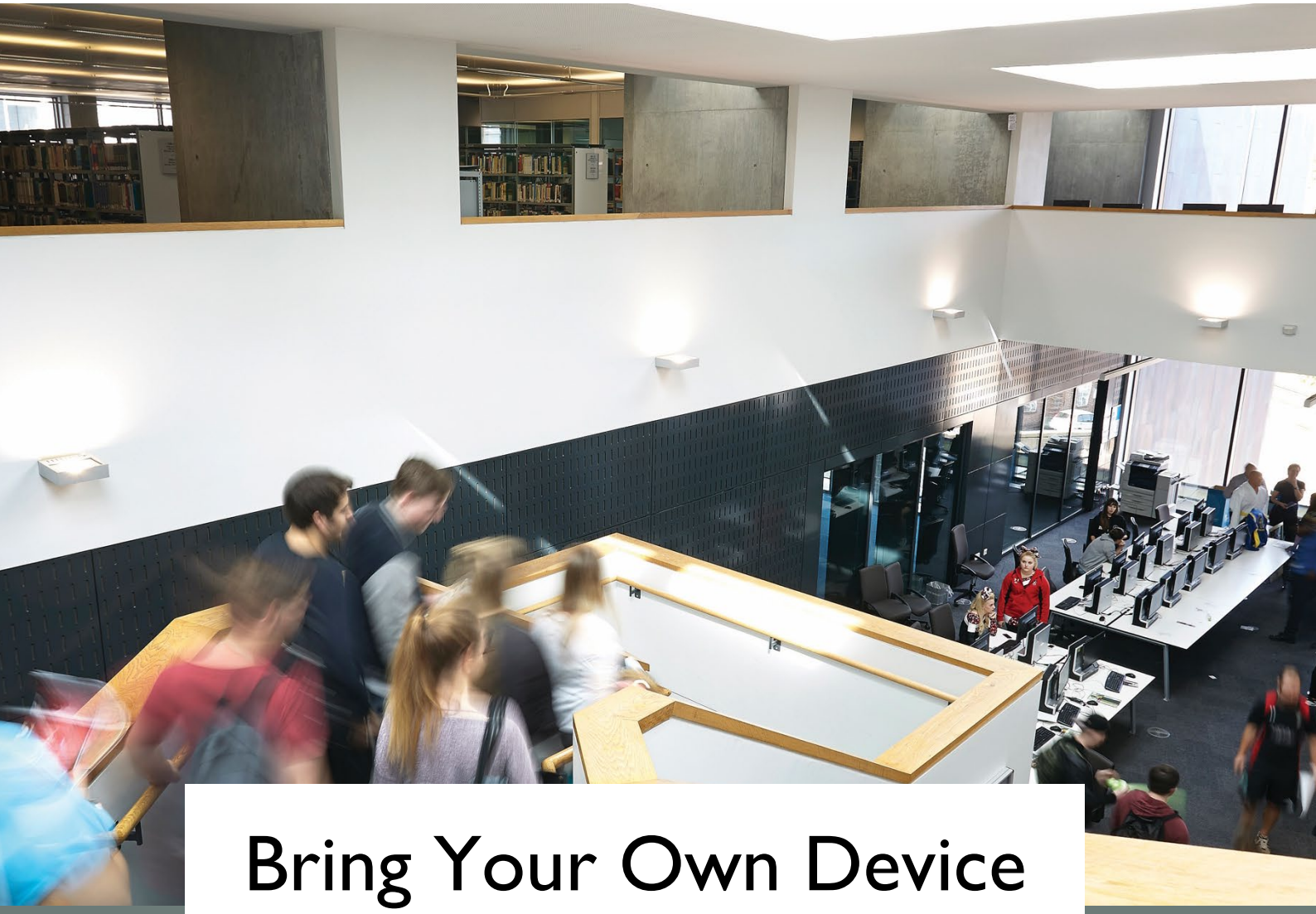
BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891



# Bring Your Own Device (BYOD) Policy

# Contents



| | | | |
|---|---|---|---|
| **Approved by:** | University Executive Team | **Date first published:** | Apr-2019 |
| **Version:** | 1.2 | **Date updated:** | Jun-2024 |
| **Owner:** | Director of DTS | **Review Date:** | Jun-2029 |

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the University Secretariat.

# Purpose

1 The University is committed to meeting its legal and duty of care obligations while at the same time providing a flexible environment to allow the use of non-University owned or issued devices to access corporate systems and store University information.

2 The use of non-University owned or issued devices for work purposes can be beneficial to the University but it also introduces new risks protecting the integrity, confidentiality and availability of University information.

3 The University does not have any control on the security mechanisms implemented on non-University owned or issued devices. Therefore if the device was compromised, lost or stolen there would be a risk that any University information stored on it could be accessed and exploited by unauthorised individuals.

4 This policy provides clear instructions on how personally owned devices, also referred to as Bring Your Own Device (BYOD), can be used in a safe and secure manner to ensure that the University complies with data protection legislation and that University information, in particular personal and sensitive information, is protected from unauthorised access, dissemination, alteration or deletion.

# Applicability and Scope

5 This policy applies to all University staff, partners, affiliates, contractors and third parties working at the behest of the University, who use a non-University managed device or their own personal device to processUniversity data. This is commonly known as "Bring Your Own Device" or BYOD.

6 For the purposes of this guidance BYOD covers non-University managed devices used to access any University information, system or service. This includes, but is not limited to: home desktop PCs, tablets (iPads etc.), smartphones, laptops, video and audio recording equipment.

7 Some devices may not have the capability to connect to University systems. The Digital and Technical Services (DTS) Directorate are not under any obligation to modify University systems or otherwise assist staff in connecting their own devices to University systems.

8 This policy should be read in conjunction with the Acceptable Use Policy, Information Security Policy and other supporting policies, procedures and standards.

# General Policy Provisions and Principles

9 The contents of University systems and University data remain University property. This covers all materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for the University or on its behalf is the property of the University, regardless of who owns the device.

10 University data and services (including email) should only be accessed from University provided and managed devices. If this is not possible then accessing University data and services (including e-mail) using a personal device must only be through the use of a University approved web interface (e.g. the online versions of Microsoft Office, Outlook on the Web, the web interfaces to OneDrive for Business, web access to corporate systems like Business Connect etc). Additional guidance is available on the staff intranet.

11 University data must never be downloaded or synchronised with personally owned devices.

12 The university reserves the right to remotely remove any University data or remove access to systems from BYOD devices.

13 In order to maintain the security of its systems and infrastructure any BYOD devices may be subject to additional compliance checking. This may include the imposition of configuration requirements for users to apply to devices, requirements to update software or the requirement to run managed security software. Any device that is considered a risk to the network will be subject to restricted access until it has been remediated.

14 University data held on personally owned devices is subject to the Freedom of Information Act and the Data Protection Act and must be processed in compliance with information related legislation and associated University policies.

15 The University reserves the right to refuse access to particular personally owned devices or software where it considers that there is a security risk to its systems and infrastructure.

16 While the DTS Directorate will always endeavour to assist colleagues wherever possible, the University cannot take responsibility for supporting non-University managed devices.

## User Responsibilities

17 All individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Make sure the device is running a current operating system, still being supported by the vendor and has the latest updates installed and operational;
- Make sure the device has anti-virus and anti-malware protection installed;
- Make sure the device has a firewall installed and enabled;
- Make sure the device is set to lock when left unattended;
- Ensure that the device is not used for any purpose that would be at odds with the University Acceptable Use Policy especially when it is on site or connected to the University network; and
- Pay for their own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs.

18 Staff using BYOD must:

- Take all reasonable steps to prevent the theft and loss of data;
- Set up passwords, passcodes, passkeys or biometric equivalents of sufficient length and complexity for the particular type of device;
- Set up remote wipe facilities if available and implement a remote wipe if they lose the device;
- Ensure that software on personally owned devices are appropriately licenced;
- Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead they should use their device to make use of the facilities provided to access information securely over the internet. More information on determining if information is 'confidential' is available on the staff intranet;
- Be aware of any Data Protection issues and ensure personal data is handled appropriately;
- Ensure that no University information is left on any personal device indefinitely and make sure any data or University apps are removed before a device is disposed of, sold or transferred to a third party.

## Monitoring and Access

19 The University will not routinely monitor personal devices. However it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both;
- Prevent a device accessing a particular system; and
- Take all necessary and appropriate steps to retrieve information owned by the University.

## Data Protection and BYOD

20 The University must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

21 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. A breach of the Data Protection Act can lead to the University facing significant fines. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the University's facilities being withdrawn, or even a criminal prosecution. For more information see the University's Data Protection Policy.

## Enforcement

22 Failure to comply with this policy may result in the revocation of access to University systems, whether through a personally owned device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, partner or affiliate, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

23 By using your device for University related purposes and unless otherwise agreed with you in a separate agreement with the University, you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.

## Key Relevant Documents

24 This policy should be read and understood in the context of other Buckinghamshire New University Policies which together form the Information Security framework. Key documents include:

- Acceptable Use Policy
- Data Protection Policy
- Information Security Policy
- Password and Multifactor Authentication Policy

# Table of Definitions

| | |
|---|---|
| Bring Your Own Device or BYOD | Refers to any non-University managed device or a user's own personal device used to access University data, systems or services. |
| IT Facilities | Hardware, software, data, network access, third party services, online services or IT credentials provided or arranged by Buckinghamshire New University. |
| IT Credentials | Your institutional login, or any other token (email address, smartcard, dongle) issued by the University to identify yourself when using IT facilities. |
| Staff | Staff are salaried members of the University or contracted individually by the University to provide a service. |
| Student | A person pursuing any course of study in the University. |
| University information | Includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media |
| University system or service | This includes access to University owned data and cloud services such as email via a mobile application or desktop application such as Microsoft 365. |
| Visitors | A visitor is anyone, not a member of staff or student, requiring access to University premises or services. |

# Appendix One: Equality Impact Assessment

| | | | | |
|---|---|---|---|---|
| 1. **What is changing and why?** | | | | |
| The purpose of the Bring Your Own Device (BYOD) policy it to provide all users with clear instructions on how they can use their own device – phone, laptop or tablet – to access University information and systems while ensuring that the University complies with data protection legislation and that information, in particular personal and sensitive information is protected from unauthorised access, dissemination, alteration or deletion.<br>This policy was first introduced in April 2019 and has been reviewed in accordance with the review schedule to ensure that it remains applicable to the changing requirements of the University. | | | | |
| **2. What do you know?** | | | | |
| The Policy addresses the need to ensure compliance with laws and regulations and the need to protect the University's information, balanced with the need to protect the rights of learners, staff and partners. Consultation has taken place with relevant stakeholders through their respective DESG member. | | | | |
| **3. Assessing the impact** | | | | |
| | **Could benefit** | **May adversely impact** | **What does this mean?** *Impacts identified from what you know (actual and potential)* | **What can you do?** *Actions (or why no action is possible) to advance equality of opportunity, eliminate discrimination, and foster good relations* |
| a) How could this affect different ethnicities? *Including Gypsy, Roma, Traveller, Showmen and Boaters, migrants, refugees and asylum seekers.* | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of their ethnicity.<br>It protects the interest of all users. | |
| b) How could this affect cisgender and transgender men and women (including maternity/pregnancy impact), as well as non-binary people? | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of gender, gender reassignment whether on maternity or paternity leave including whether the woman is pregnant or is/has previously been absent due to maternity leave.<br>It protects the interest of all users. | |
| c) How could this affect disabled people or carers? *Including neurodiversity, invisible disabilities and mental health conditions.* | ☒ | ☐ | Could benefit<br>This policy could be beneficial to users with disabilities who are already satisfied and familiar with the accessible devices they already own. | The policy is available on the BNU website therefore is available in different fonts, text size and through assistive technology. |
| d) How could this affect people from different faith groups? | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of religion or belief.<br>It protects the interest of all users. | |
| e) How could this affect people with different sexual orientations? | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of sexual orientation.<br>It protects the interest of all users. | |

| | | | | |
|---|---|---|---|---|
| f) How could this affect different age groups or generations? | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of age.<br>It protects the interest of all users. | |
| g) How could this affect those who are married or in a civil partnership? | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of marital status.<br>It protects the interest of all users. | |
| h) How could this affect people from different backgrounds such as: socio-economic disadvantage, homeless, alcohol and/or substance misuse, people experiencing domestic and/or sexual violence, ex-armed forces, looked after children and care leavers. | ☐ | ☐ | Neutral impact<br>This policy applies to all regardless of socio-economic background.<br>It protects the interest of all users. | |
| i) How could this affect people with multiple intersectional experiences? | ☐ | ☐ | Neutral impact<br>This policy applies to all in the same way therefore there is no cumulative impact on users. | |

| **4. Overall outcome** | | | |
|---|---|---|---|
| No major change needed ☒ | Adjust approach ☐ | Adverse impact but continue ☐ | Stop and remove ☐ |

**5. Details of further actions needed**

All staff will be made aware of the updated policy via an announcement;
The policy will be made available to all staff as link on the staff intranet;
All students will be made aware of the updated policy via MYBNU;
The policy is accessible to all users as a PDF document on the BNU web site;
The inappropriate use of the Policy will be managed in accordance with the University's policies and procedures and reported to external bodies when appropriate.

**6. Arrangements for delivery and future monitoring**

The policy will be reviewed every three years to ensure that it still meets the requirements of the University and Data Protection Regulations. Any changes to data protection legislation and analysis of the policy in practise will inform future changes.
The Director of Digital & Technical Services is responsible for reviewing the policy on an annual basis.

| | | | | |
|---|---|---|---|---|
| **7. Completed by:** | Jenny Horwood | Technical Project Manager | **Date** | 25-January-2023 |
| **8. Signed off by:** | Nicholas Roussel-Milner | Director DTS | **Date** | 27/02/2023 |

**High Wycombe Campus**
Queen Alexandra Road
High Wycombe
Buckinghamshire
HP11 2JZ

**Aylesbury Campus**
59 Walton Street
Aylesbury
Buckinghamshire
HP21 7QG

**Uxbridge Campus**
106 Oxford Road
Uxbridge
Middlesex
UB8 1NA

**BNU based at Pinewood Studios**

Pinewood Studios
Pinewood Road
Iver Heath
Buckinghamshire
SL0 0NH

**Missenden Abbey**
London Road
Great Missenden
Buckinghamshire
HP16 0BD

Telephone: 01494 522 141

BucksNewUni

BucksNewUni

BucksNewUni

BucksNewUniversity

If you have any queries about this policy, please contact the School or Directorate responsible for the policy