Bring Your Own Device (BYOD) Policy

Introduction

1. Northeastern University London (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 were compromised, lost or stolen there would be a risk that any University information stored on it could be accessed and exploited by unauthorised individuals.

Scope

4. This Policy applies to all University staff, students, 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 process University data. This is commonly known as “Bring Your Own Device” or BYOD.
5. For the purposes of this Policy, non-University managed or personal devices include, but are not limited to: home desktop PCs, tablets (iPads etc.), smartphones, laptops, video and audio recording equipment.
6. Some devices may not have the capability to connect to University systems. The IT Department are not under any obligation to modify University systems or otherwise assist staff in connecting their own devices to University systems.
7. This Policy should be read in conjunction with the Data Protection Policy and its supporting policies, procedures and standards.

Intent

8. This Policy is produced to provide a clear instruction on how BYOD devices can be used in the University to ensure that the University complies with data protection legislation and that University information, in particular personal and sensitive information, is protected from unauthorized access, dissemination, alteration or deletion.

Provisions and Principles

General

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, and is the property of the University, regardless of who owns the device.
10. 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.
11. 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.
12. While the IT Department will always endeavour to assist colleagues and students wherever possible, the University cannot take responsibility for supporting non-University managed devices.

User Responsibilities

13. All individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:
    - 13.1. Familiarise themselves with their device and its security features so that they can ensure the safety of University information (as well as their own information);
    - 13.2. Invoke the relevant security features for the device;
    - 13.3. Maintain the device themselves ensuring it is regularly patched and upgraded using updates provided by vendors;
    - 13.4. Ensure that the device is not used for any purpose that would be at odds with the University IT regulations of use especially when it is on site or connected to the University network; and
    - 13.5. 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.
14. Staff using BYOD must take all reasonable steps to:
    - 14.1. Prevent theft and loss of data;

14.2. Keep information confidential where appropriate;

14.3. Maintain the integrity of data and information, including that on campus; and

14.4. Take responsibility for any software they download onto their device.

15. Staff using BYOD must:

15.1. Set up passwords, passcodes, passkeys or biometric equivalents of sufficient length and complexity for the particular type of device;

15.2. Set up remote wipe facilities if available and implement a remote wipe if they lose the device;

15.3. Ensure that software on personally owned devices is appropriately licenced;

15.4. Encrypt documents or devices as necessary;

15.5. 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 University’s web site);

15.6. 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, including information contained within emails;

15.7. Ensure that relevant information is copied back onto University systems and manage any potential data integrity issues with existing information;

15.8. Report the loss of any device containing University data (including email) to the IT Department;

15.9. Be aware of any Data Protection issues and ensure personal data is handled appropriately;

15.10. Report any security breach immediately to the Data Protection Officer in accordance with the University’s Data Protection Policy;

15.11. Ensure that no University information is left on any personal device indefinitely and make sure data is removed before a device is disposed of, sold or transferred to a third party; and

15.12. Not keep any information longer than is necessary and only in line with the Data Retention Schedule set out in the University's Data Protection Policy.

Monitoring and Access

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

    16.1. Prevent access to a particular device from either the wired or wireless networks or both;

    16.2. Prevent a device accessing a particular system;

    16.3. Take all necessary and appropriate steps to retrieve information owned by the University.

Data Protection and BYOD

17. 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.

18. 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

19. 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.

20. 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.

Version History

Title: Bring Your Own Device (BYOD) Policy **Approved by: Executive Committee** **Location: Academic Handbook/ Data Protection**				
Version Number	**Date Approved**	**Date Published**	**Owner**	**Proposed Next Review Date**
1.1	September 2022	September 2022	Director of Resourcing and Operations	September 2023
1.0	September 2022	September 2022	Director of Resourcing and Operations	September 2023
Related Documents	Data Protection Policy; Information Security Policy; Acceptable Use Policy for Students (IT)			
External Reference Point(s)	Data Protection Act 2018; Freedom of Information Act			