Personal Device (BYOD) Policy

Document Reference: IT-POL-102

Document Classification: Policy

Data Classification: Public

Version number: 1.0

Relevant CIS Control(s): 4.3, 4.5-4.8, 4.10, 4.11, 9.1-9.7, 10.1, 10.2

Status: Approved

Approved by (Board): University Leadership Team

Approval date: 03 June 2025

Effective from: 03 June 2025

Review Frequency: Annual

Next review date: 03 June 2026

Document author: Cyber Security

Document owner: Director of Technology

Contact: IT Services

Collaborative provision: No

State whether this document is applicable to the University's collaborative partners

Related documents: Managed Device Policy, Acceptable Use Policy, Software Usage Policy, Data Protection Policy, Information Governance and Assurance Policy, Information Security Controls Policy and sub-policies

University document: No

A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location: hull.ac.uk

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.
- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.
- This document is available in alternative formats from policy@hull.ac.uk.

Personal Device (BYOD) Policy

Table of Contents

1 INTRODUCTION 3
2 SCOPE 3
3 PERSONAL DEVICE (BYOD) POLICY 4
4 MICROSOFT INTUNE POLICY 6
5 GLOSSARY OF TERMS 8
6 RESPONSIBLE, ACCOUNTABLE, CONSULTED, AND INFORMED (RACI) MATRIX 11
7 VERSION CONTROL 11

Personal Device (BYOD) Policy

1 Introduction

1.1 It is critical that the University can safeguard its *IT resources* and *organisational data*. This is done by placing security controls on devices that are used to access services, systems, and information.

1.2 The University promotes and understands the benefits of information technologies to enable its members to achieve their academic and business objectives, however, this must be balanced against the University acting as a Data Controller and Data Processor under Data Protection law when it comes to the appropriate and secure handling and processing of information.

1.3 The security controls in place on university devices have been implemented to allow users to conduct their work or research tasks in a secure way. These controls should not be seen as blockers preventing a user from conducting their work or research. If a user is unable to perform their work or research, they should seek advice from IT Services.

1.4 This policy supports the overarching **Information Security Controls Policy** and its sub-policies as well as the **Data Protection** and **Information Governance and Assurance** policies.

1.5 A glossary of technical terms, which are defined in pink, underlined, and italicised, can be found at the end of this policy. Clicking on each term will take you to its definition.

2 Scope

2.1 This policy, and all policies referenced herein, shall apply to all members of the University community, including faculty, students, administrators, staff, alumni, authorized guests, delegates, and independent contractors (the "End user(s)" or "you") who use a *personal device* to access University of Hull resources, systems, and data.

2.2 A *personal device* is also known as *'Bring your own device' (BYOD)*, and these terms are used interchangeably throughout this policy. Figure 1, below, provides examples of the types of end-user devices.

2.3 A *managed device* should be used in the first instance. Should there be a legitimate reason to use a personal device for university purposes, authorisation is required from IT Services. The end user must agree to the terms set out in this policy for authorisation to be granted.

2.4 This policy does not relate to university-owned IT devices for guidelines regarding these devices, refer to the dedicated **Managed Device Policy**.

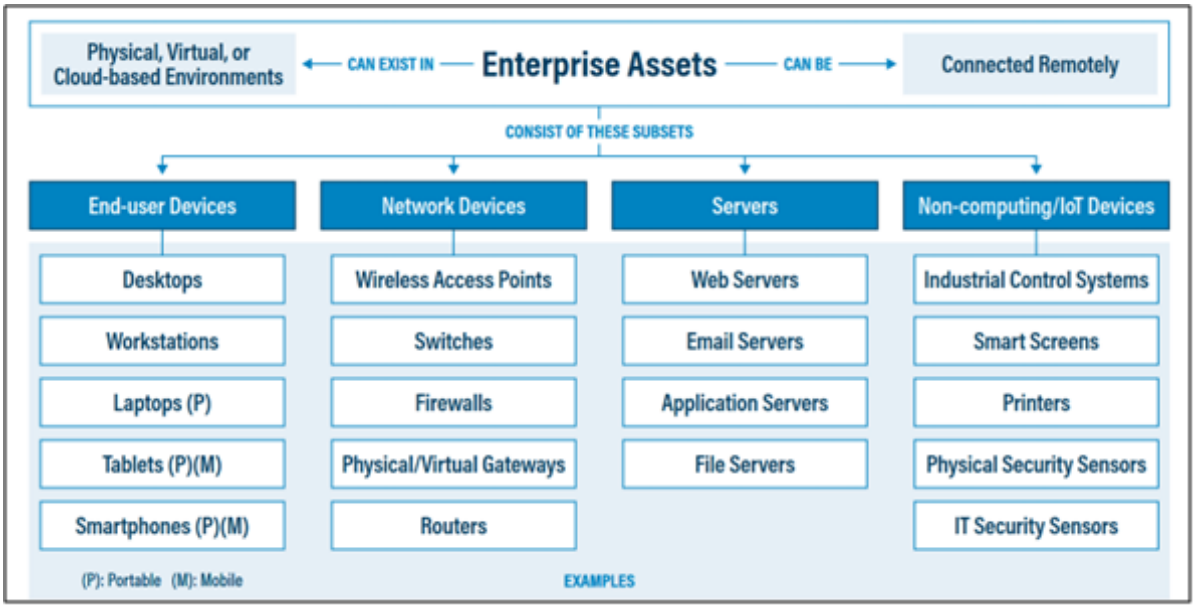

Figure 1: Enterprise Asset definition according to CIS Controls v8

3 Personal Device (BYOD) Policy

3.1 *Personal devices* may not have the capability to access certain University information and systems.

3.2 Similarly, not all organisational data may not be available to end users using a *personal device* depending on its classification, according to the **Data Classification and Handling Policy**.

3.3 Unauthorised software, as defined in the **Software Usage Policy**, must not be used in conjunction with *organisational data*.

3.4 IT Services are under no obligation to modify systems or the network, or to assist those with *personal devices*, to be able to do so.

3.5 *Personal devices* will be placed onto the University's Untrusted Network.

3.6 End users must confirm that they are the only user of the *personal device*. If the device is used by multiple individuals, this poses a data protection and cyber-security risk as *organisational data* may be inadvertently breached, or malware may be introduced into the University networks, for example.

3.7 If a *personal device* is used to access University *organisational data* and systems, the owner must ensure the device meets the minimum security measures, including but not limited to:

- Familiarising themselves with their device and its security features to ensure the security of university information.
- Taking all reasonable steps to prevent theft, cyber-attacks, and loss of data whilst upholding the wider University policies including but not limited to:
    - Acceptable Use Policy.
    - Software Usage Policy.
    - Data Protection Policy.
    - Data Retention Policy.
    - Data Breach Policy.
    - Password and Multi-Factor Authentication Policy.
    - Data Classification and Handling Policy.
- The latest versions of these policies can be found on the University website.
- Controlling access to the device either through fingerprint or biometric scanning, password, or PIN.
- Ensuring that a device or screen lock is enabled after a period of inactivity (no longer than 15 minutes is recommended).
- Enabling a 'remote wipe' capability if the device supports it.
- Keeping the device operating system, operating system security updates, and any installed applications updated, particularly ensuring that any critical security updates have been applied.
- It is recommended that these updates and patches are set to automatically download and install.
- Not using a device that has been illegally licenced (i.e., 'jailbroken' or 'rooted') as this can compromise the integrity of the security of the device.

3.8 When using a personal (home) network, Cyber Security recommend that the Wi-Fi router's administrator password should be changed from its default. Additionally, the router's security configuration should be kept up to date by installing updates; it is recommended that these updates are set to automatically download and install.

3.9 When using a *public network*, the user should assume the network is insecure and untrusted, and therefore not perform any tasks that require sensitive information, for example financial or *personal identifiable information (PII)*.

3.10 If the device is lost, sold, or stolen the end user must report it to IT Services.

3.11 Upon leaving the University or the device changing ownership (i.e., being sold), the staff member must ensure any University data or email configurations are securely wiped.

3.12 The **Software Policy** outlines what software has been authorised for use when accessing University data, and end-users should familiarise themselves with this policy.

3.13 A range of technical controls will be implemented by IT Services to ensure that personal devices are compliant with this policy.

3.14 IT Services will not monitor the content of *personal devices (BYODs)*, but will obtain the following information for audit purposes, for example:

- Device name
- Operating system
- Operating system version
- Logon data

3.15 If a security incident occurs IT Services reserve the right to disable associated devices and user accounts from accessing the University network and systems without notice.

4 Microsoft Intune Policy

4.1 Undergraduate students who use personal mobile devices are exempt from this section of the policy.

4.2 The university has deployed *Microsoft Intune* for the sole purpose of allowing end users to use their *mobile devices* for university purposes. Figure 1, in section 2: Scope, shows that only smartphones and tablets are classed as a mobile device.

4.3 Personally owned and University-owned laptops are not currently in scope for Intune use.

4.4 End users who register their mobile device for Intune must agree to[1]:

- Ensure that their *mobile device*'s *operating system* is still being supported by the vendor.
- Requiring a 6-digit pin, as a minimum, to unlock the device.
- Use biometrics (e.g., the use of a fingerprint or face) where possible, to unlock the device, requiring a 6-digit pin as an alternative.
- Enabling automatic device locking when it is not in use.
- Install security updates within 14 days of them becoming available.
- Only install applications (apps) from the manufacturers respective store (e.g., Apple's App Store, or the Google Play Store).
- Uninstalling unused apps.
- Not using a 'rooted' or 'jailbroken' device.
- Enabling the 'remote wipe/erase' function, where possible.
- Report their device, if it becomes lost or stolen, to IT Services.

4.5 End users must take all reasonable steps to prevent theft, cyber-attacks, and loss of data whilst upholding the wider University policies relating to:

[1] https://ce-knowledge-hub.iasme.co.uk/space/CEKH/2651652226/Guidance+to+BYOD

- Acceptable Use Policy.
- Software Usage Policy.
- Data Protection Policy.
- Data Retention Policy.
- Data Breach Policy.
- Password and Multi-Factor Authentication Policy.
- Data Classification and Handling Policy.

4.6 It is vital that end-users understand that the University will be able to view some data that attributes a device to an individual[2], including:

- Device owner
- Device name
- Device serial number
- Device model
- Device manufacturer
- Operating system and version
- Device IMEI
- Last four digits of your phone number

4.7 Conversely, the University will not be able to view[2]:

- Calling and web browsing history
- Personal emails and text messages
- Contacts
- Calendar
- Passwords
- Pictures, including what's in the photos app or camera roll
- Content of user created documents

4.8 Further information can be found on the Support Portal, including how to register your *mobile device* for Intune.

[2] https://learn.microsoft.com/en-us/mem/intune-service/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune

5 Glossary of Terms

5.1 *Bring your own Device (BYOD) / Personal Device* = BYOD is a concept that allows end users to use their own personally owned device for organisational purposes. Whilst the device is the sole responsibility of the end user, it is important to remember that the University still owns the organisational data and resources that are used to complete the business function[3].

5.2 *IT Resources* = Also known as an enterprise asset, these refer to a resource, owned by an enterprise (the University of Hull), with the potential to process or store data[4]. These include computing, networking, communications, application, and tele-communications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

5.3 *Managed Device* = An end-user device that is owned by the University and is installed with a standardised image, for adherence to security best practice, as outlined in the **Information Security Controls Policy** and its sub-policies. These devices provide individuals with a consistent experience which is supportable and meets the compliance requirements of the organisation and its partners. These devices will meet the requirements for most end-users and are able to provide the highest assurance level.

5.4 *Microsoft Intune* = A cloud-based management solution for end-user devices that manages access to *organisational data* and resources. This solution can be implemented on *managed devices*, via Intune for *mobile device management (MDM)*, as well as *BYOD devices*, via Intune for *mobile application management (MAM)*[5].

5.4.1 *Mobile Application Management* = Often referred to as MAM, this approach allows the University to define and centrally manage security and data compliance policies to protect application data regardless of the device that is being used [7] [6]. This balances the usability of BYODs against securing *organisational data* and minimising data breaches.

[3] https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
[4] CIS Controls Acceptable Use Policy Template (https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)
[5] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
[6] https://www.trio.so/blog/mobile-application-management/

5.4.2 *Mobile Device Management* = Also known as MDM, this is a device-centred management approach[7]. MDM is a more in-depth approach when compared to *Mobile Application Management (MAM)* in that MDM can manage device configuration, device features and infrastructure services in addition to application (and therefore *organisational data*) management[7]. This approach allows the University to define and centrally manage cyber-security and data compliance policies in more depth, compared to MAM solutions. Given that the university has full control on the security controls baselines that are implemented, MDM is used to provide a higher level of assurance on devices that have been recognised as accredited.

5.5 *Mobile Device* = works without need for a physical connection (i.e., power supply) since they have their own self-contained power source, have their own non-removable data storage, and can be easily carried by one individual[8].

5.6 *Operating System* = An OS manages *all* software and hardware on a computing device. Usually there are several different resources (e.g., computer programmes or processes) running at the same time, and they all need to access the computing device's *central processing unit (CPU)*, as well as computing memory and storage[9]. The operating system, then, coordinates all these resources to ensure that the flow of information remains constant. Most computing devices provide user interfaces (either graphically, or through a command-line) and would not be able to function without an OS[10].

5.6.1 *Central Processing Unit* = Also known as a CPU, processor or microprocessor, this is the part of a computer that can interpret and execute instructions[11]. A CPU is the control centre, or 'brain', of a computing device. Some devices may have multiple processors making them more powerful than other devices with only a single processor.

5.7 *Organisational Data* = Data owned by the university; this can include any research data, office documents, financial data, and even email.

[7] https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management
[8] https://csrc.nist.gov/glossary/term/mobile_device
[9] https://edu.gcfglobal.org/en/computerbasics/understanding-operating-systems/1/#
[10] https://www.gartner.com/en/information-technology/glossary/os-operating-system
[11] https://www.gartner.com/en/information-technology/glossary/cpu-central-processing-unit

5.8 *Personal Identifiable Information (PII)* = Also known as 'personal data' PII refers to any information relating to an identified or identifiable person ('data subject'). An identifiable person is one who can be identified – directly or indirectly – by reference to an identifying characteristic; for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person[12].

5.9 *Public network* = Also known as a wide area network (WAN)[13] or the internet, this network is accessible by virtually anyone and can cover a large geographical area. These networks are easily accessible and designed for convenience, but they are also more vulnerable to interference, congestion, cyber-attacks, and malware. These types of networks are commonly available in restaurants, cafes, and airports, for example[14]. At the University of Hull, our public network refers to services that are accessible over the internet, with no requirement to connect to our VPN, for example, the University's website.

[12] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/
[13] https://purple.ai/blogs/whats-the-difference-between-a-lan-and-a-wan/
[14] https://www.digi.com/blog/post/private-network-vs-public-network

6 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

6.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[15]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[16]. A brief definition of each role is given in the table below.

6.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

	Definition	Role
Responsible (R)	Answerable for the correct completion of the task	End User Services
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Director of Technology
Consulted (C)	Provide input based on how this will impact their domain of expertise	Information Governance Committee
Informed (I)	Those who are kept up to date on progress	University Leadership Team

7 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Hollie Felice, Carl McCabe, Nigel Kavanagh	08 May 2025	All

[15] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[16] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/