Managed Device Policy

Document Reference: IT-POL-101

Document Classification: Policy

Data Classification: Public

Version number: 3.0

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: Personal Device (BYOD) Policy, Acceptable Use Policy, Software 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: Public website (www.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.

Managed Device Policy

Table of Contents

Managed Device Policy

1 Introduction

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

1.2 The University promotes the use of information technologies to support its members in achieving their academic and business objectives. However, this must be balanced with the University's responsibility to ensure that all information, whether personal, sensitive, or institutional, is handled and processed securely and appropriately. Where personal data is involved, the University must also meet its obligations as a Data Controller and Data Processor under Data Protection law.

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 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 University-owned *managed device* or *unmanaged device*. This includes those who are working remotely as well as on campus.

2.2 University-owned end-user devices, that are classed as managed, will have the highest assurance level and are suitable for most staff. Unmanaged devices, however, will provide the lowest assurance level and will only be issued in cases where a managed device is deemed as inappropriate for the given business purpose.

3 Purpose

3.1 This policy does not relate to *Personal Devices (BYODs)*, for guidelines regarding these devices, refer to the dedicated **Personal Device (BYOD) Policy**.

3.2 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**.

4 Risks

4.1 *Data Protection:* The University is bound by Data Protection legislation that specifies that technical and organisational measures shall be taken to safeguard personal data from loss, destruction, or damage.

4.2 *Compromise:* Unmanaged devices create challenges and risks around security that need to be managed effectively to protect the University network, its managed systems, and the data held within such systems.

5 Responsibilities

5.1 This section outlines the responsibilities within IT Services, as well as the responsibilities of an end-user, when using a University end-user asset.

5.2 IT Services:

5.2.1 Shall monitor the usage of end-user assets to ensure they remain compliant with approved baseline configurations.

5.2.2 Will ensure that security updates ('patches') on operating systems, and approved applications, are being routinely installed – unless an alternative approved patching process is used.

5.2.3 Shall ensure that high and critical risk security updates, on operating systems, firmware, and approved applications, are installed within 14 days of being released.

5.2.4 Will ensure that authorised software that is no longer being supported with security updates is removed and replaced in a timely manner, as per the Software Policy.

5.2.5 Reserve the right to remove any software that has not been authorised as per the Software Policy.

5.2.6 Will isolate a device upon a user leaving the university, or upon a device being reported as lost or stolen.

5.2.7 In the event of a security incident, IT Services reserve the right to disable associated devices, and user accounts, from accessing the University network and resources without notice.

5.3 End-Users:

5.3.1 Must familiarise themselves with their device and its security features to ensure the security of university information.

5.3.2 Must take all reasonable steps to prevent theft and loss of data, and uphold the wider University policies, including but not limited to:

- Acceptable Use Policy.
- Software Usage Policy
- Information Security Controls Policy
- Data Protection Policy.
- Data Classification and Handling Policy.
- Data Retention Policy.
- Data Breach Policy.

The latest versions of these policies can be found on the University website (www.hull.ac.uk).

5.3.3 Must not disable or modify the update frequency of anti-malware software on their enterprise assets.

5.3.4 Shall not amend the configuration of a managed device, as stated in the Acceptable Use Policy. For instance, by modifying the frequency of operating system updates.

5.3.5 Is responsible for any software they have been authorised to install on their device – including keeping software up to date and removing the software when it is no longer required – as per the **Software Usage Policy**.

5.3.6 Upon leaving the university, or upon the completion of research, must return all University *managed device* to IT Services.

5.3.7 In cases where a newer *managed device* has been issued, the old device must be returned to IT Services.

5.3.8 If a *managed device* is lost or stolen the device owner must report it to IT Services at the earliest opportunity.

5.3.9 Must be aware that only *managed devices* can be fully assured for the purposes of accreditation when used to fulfil the requirements for research projects, grants, and tenders.

6 Managed Device Policy

All members of university staff are required to use a *managed device* to conduct University business.

6.1 Requests for a *managed device* can be submitted through the Support Portal via this form.

6.2 End-user *managed devices* and applications, are configured according to vendor-provided or industry hardening requirements. These devices will have the following configuration, as a minimum:

- Enrolment into an asset management system, including a *mobile device management* solution
- Placed onto the University's trusted network
- Automatic session expirations (screen lockouts) for less than 15 minutes
- *Mobile devices* will have automatic session expirations configured to less than 2

minutes
- A host-based *firewall*
- Access to University resources via a *Virtual Private Network (VPN)*
- *Endpoint Privilege Management (EPM)*
- Appropriately disabled or configured default accounts to prevent unauthorized access (e.g., unauthorized password change)
- Automatic updates enabled for operating systems, and approved software, unless an alternative approved patching process is used
- Only software that has been authorized, as per the **Software Usage Policy**, including but not limited to:
    - Web browsers
    - Web browser extensions
    - Email clients
    - Office applications
    - Disabled autorun and autoplay functions on operating systems on removable media.
    - Anti-malware software, where applicable:
        - Anti-malware software is configured to automatically update.
        - As part of the university's defence in-depth approach to security, anti-malware protection is also implemented on our email servers.

6.3 When using a personal (home) network, the 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.

6.4 When using a *public network*, the user should assume the network is insecure and untrusted, and therefore not perform any tasks that access or require sensitive information, for example financial or *protected information*.

7 Unmanaged Device Policy

7.1 The use of university-owned *unmanaged devices* – will only be approved as an exception for extremely specific needs, and where a managed device is assessed as unsuitable.

7.2 Requests must be made via the Support Portal and must specify:

- The reason for the request – including why a managed device cannot be used.
- The risk(s) to the University (e.g., data loss, data breach, cyber-attack).
- How the device will be appropriately secured.
- A review date.

7.3 An unmanaged device must still be enrolled onto some IT management systems to ensure compliance with this policy:

- Enrolment into an asset management system, including a *mobile device management* solution.

- A host-based *firewall*
- Anti-malware software

7.4 *Unmanaged device* requests will be made on a case-by-case basis and must be agreed through Cyber Security within IT Services.

7.5 In addition to the provided review date, Cyber Security will conduct periodic reviews to ensure compliance with this policy, and they reserve the right to revoke access to the device.

7.6 When the *unmanaged device* is no longer required, it must be returned to IT Services.

8 Glossary of Terms

8.1 *Endpoint Privilege Management* = Often referred to as EPM, this is a solution that manages temporary privileged access to devices. An end user needs to request privileged access, which must be approved, ahead of being able to perform privileged actions on a device[1]. This helps to balance usability with cyber security by ensuring that end users can still carry out university business in a secure manner. At the university, EPM is commonly used so that an end user can install bespoke software, to support their work and/or studies, that is not managed via IT Services. End users then become responsible for ensuring this software is kept up to date and in support and are responsible for removing the software when it is no longer required.

8.2 *Firewall* = A network device that is placed on a network's boundary and inspects traffic (network requests to access a website, for example), to determine whether the traffic is allowed to pass through the firewall, based on defined rules. A firewall is commonly placed at the edge of an internal network (i.e., intranet) to inspect requests coming in from outside the internal network (i.e., the internet). A firewall may also be placed within an internal network, by enforcing different rules, for example to restrict different devices (e.g., printers and CCTV cameras) from being able to interact with one another.

[1] https://www.oneidentity.com/what-is-endpoint-privilege-management/

8.3 *Managed Device* = 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 data2. A managed device 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.

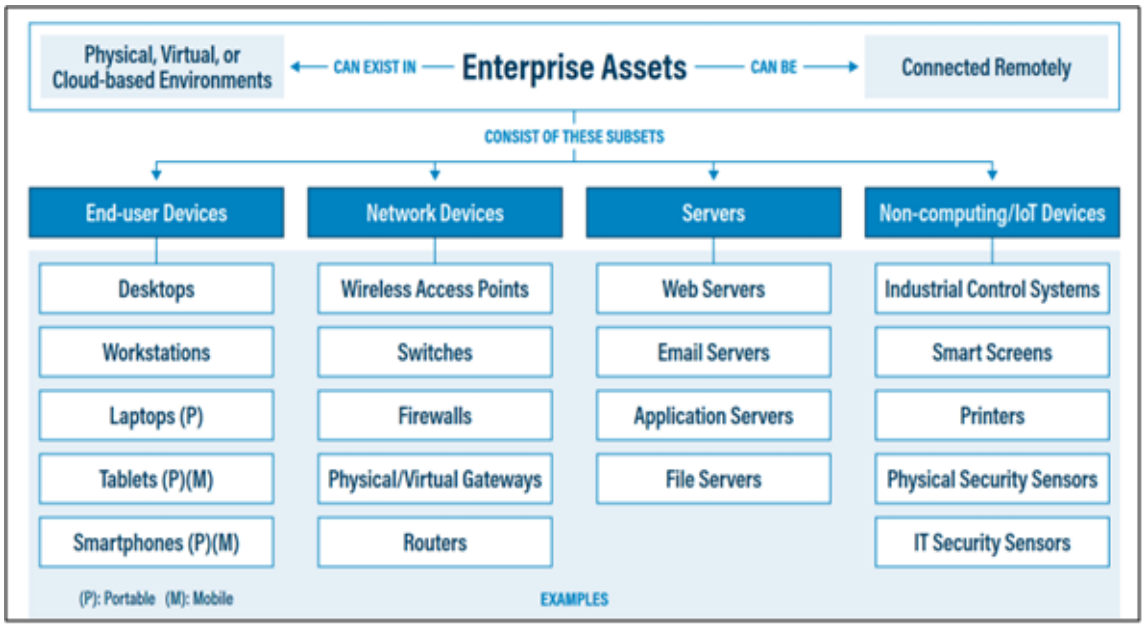

Figure 1: Enterprise Asset Definition according to CIS Controls v8

8.4 *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[3].

[2] CIS Controls Acceptable Use Policy Template (https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)
[3] https://csrc.nist.gov/glossary/term/mobile_device

8.5 *Mobile Device Management* = Also known as MDM, this is a device-centred management approach[4]. 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[5]. 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.

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

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

8.6 *Operating System* = An operating system (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[8]. 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[9].

8.6.1 *Central Processing Unit* = Also known as a CPU, processor or microprocessor, this is the part of a computer that can interpret and execute instructions[10]. 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.

[4] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
[5] https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management
[6] https://www.trio.so/blog/mobile-application-management/
[7] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
[8] https://edu.gcfglobal.org/en/computerbasics/understanding-operating-systems/1/#
[9] https://www.gartner.com/en/information-technology/glossary/os-operating-system
[10] https://www.gartner.com/en/information-technology/glossary/cpu-central-processing-unit

8.7 *Protected Information* = Information that falls under the scope of the **Data Protection Act** or **UK General Data Protection Regulations (UK GDPR)**, as well as other types of sensitive or confidential information. This may include *Personally Identifiable Information (PII)*, which can be used to identify an individual, or any data deemed confidential for operational, legal, or academic reasons. Safeguarding the security of protected information is a complex issue, with organisational, technical, and human aspects. University policies and guidelines on Data Protection and Information Assurance are available on the University website.

8.7.1 *Personally Identifiable Information* = 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[11].

8.8 *Public Network* = Also known as a wide area network (WAN)[12] 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[13]. 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.

8.9 *Unmanaged Device* = An end-user device that is owned by the University but does not have a standardised image installed upon it. These devices will still be subject to some monitoring from IT Services; for example, enrolment onto the asset inventory platform. The primary owner (end-user) of the device, however, will be responsible for safe keeping of the device and ensuring the device remains up to date. The eligibility for these devices is dependent upon the requirements, and users must outline why a managed and co-managed device are unsuitable, but all requests must be made to IT Services via the Support Portal.

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

8.10 *Virtual Private Network* = Commonly referred to as a VPN, these provide secure connectivity between devices in physically separate locations[14]. This allows for secure access to university resources, even when not physically on campus, and decreases unauthorised access attempts.

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

9.1 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.

9.2 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	IT Services End Users *(as specified in the responsibilities section)*
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

[14] https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks
[15] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[16] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/

10 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Steph Jones, Nigel Kavanagh	11 October 2021	All
2.0	Hollie Huxstep, Carl McCabe, Nigel Kavanagh	19 February 2024	All
3.0	Harry Steggles, Hollie Felice, Carl McCabe, Nigel Kavanagh	08 May 2025	All