UNIVERSITY of HULL

Mobile and Remote Working Policy

Document Reference:	IT-POL-103
Document Classification:	Policy
Data Classification:	Public
Version number:	4.0
Relevant CIS Control(s):	12.7, 13.5
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:	Information Governance and Assurance Policy Data Protection 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:	University Website

- 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.

Mobile and Remote Working Policy

Table of Contents

Mobile and Remote Working Policy

1 Introduction

1.1 Mobile working and remote access extend the transit and storage of information (or operation of systems) outside of the organisational infrastructure, typically over the Internet. This brings about great benefit to the University in terms of its ability to meet its objectives but also exposes it to new risks that must be managed effectively.

2 Purpose

2.1 This policy outlines the risks associated with mobile working and remote access to systems and describes the responsibilities of Information System/Asset Owners in terms of authorising mobile and remote working, including enabling remote access for third parties or service providers.

2.2 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**.

2.3 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.

3 Scope

3.1 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 the University's *IT Resources* remotely.

3.2 This policy covers all University information and systems being accessed electronically from remote locations, or via mobile devices.

3.3 For the purposes of this policy, the terms *"mobile"* and *"remote"* are used interchangeably and should be taken to cover any scenario where University related business is carried out away from campus or the campus network.

3.4 This policy focuses on portable and *mobile devices*.

4 Risks

4.1 **Loss or theft of the device:** *Mobile devices* are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations. Therefore, steps must be taken to keep mobile devices as secure as possible, and to not leave mobile devices unattended.

4.2 **Being overlooked:** Some users may work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials including passwords. Care must be taken to ensure that *organisational data*, including *personal identifiable information (PII)*, cannot be viewed by onlookers, or those passing by.

4.3 **Loss of credentials:** If user credentials (such as username, password, or MFA factor) are stored within a device used for remote working, or remote access, and it is lost or stolen, the attacker could access and use those credentials to compromise services or information stored on (or accessible from) that device. If this occurs, reset all affected user account passwords and contact IT services.

4.4 **Unauthorised access to remote gateways:** Credentials that are stolen via other attacks (such as phishing) may be used by attackers to gain unauthorised access to interfaces that are exposed to the Internet, such as email, student, or HR systems. This can potentially compromise any information stored within those systems.

4.5 **Tampering:** An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor user activity on the device, including authentication credentials.

5 Policy

5.1 Managers and information asset owners shall ensure that corresponding processes are in place to authorise remote access and mobile working within their area of responsibility.

5.2 Where third parties have been permitted to access University *IT resources* remotely, risk owners should ensure that appropriate contracts are in place to cover such access, and that said contracts are regularly reviewed to ensure compliance with this and other information security policies such as the **Information Governance and Assurance Policy** (those designated as Information System Owners should work to ensure this).

5.3 University staff members working on a mobile or remote basis should ensure that they are authorised to do so, and that access is in accordance with this policy.

5.4 Similarly, *mobile devices* that are to be used, must also be appropriately authorised to access organisational data.

5.5 *Mobile devices* that are to be used when working away from campus must still be in support and receive operating system (OS) updates, by the vendor.

5.6 Consideration must be given to the supported security features available on a *mobile device's* hardware.

5.7 University and staff-owned mobile devices shall be registered in a *Mobile Device Management (MDM)* or *Mobile Application Management (MAM)* platform, respectively, where they must:

- Be inventoried for traceability and auditing purposes.
- Be classified according to the information that is stored on devices.
- Use the secure version of a device when available.
- Have undergone vendor due diligence, regarding security reputation. This applies to hardware and software vendors.
- Only be authorised to install approved software applications, for business purposes.
- Meet the defined minimum security controls baselines, to access organisational data.
- Support the forcing of remotely wiping (deleting) *organisational data* only, when required.
- Be used mostly for business purposes; limited personal use is permitted, as outlined in the **Acceptable Use Policy**.

5.8 Where devices do not currently meet the required security controls baselines, they must be brought up to date as soon as possible, in accordance with cyber security accreditation requirements.

5.9 *Mobile devices* that fail to meet the minimum-security controls baselines must have their access to organisational data restricted and/or removed according to the following:

- Maximum PIN attempts = 5
- Requirement to reauthenticate = 24 hours offline
- Remote wiping of data = 90 days offline
- If a university user account is disabled = access to *MAM* is blocked.

5.10 University-owned *mobile devices* must be kept secure, and not left unattended or on display in public, or in cars, for example.

5.11 Likewise, when working in a public space, consideration must be taken to avoid being overlooked when accessing *organisational data*, for example.

5.12 Users engaging in mobile and remote working shall adhere to the University's **Acceptable Use Policy** and ensure that their working practices keep *IT resources* protected from unauthorised access, or data breaches, for example.

5.13 To ensure the confidentiality, integrity, and availability of university *IT resources*, only approved technologies may be used for remote access and mobile working. This includes, but is not limited to, using the approved connection methods and collaboration software, for example using a VPN or secure HTTP (HTTPS) to access *organisational data*.

5.14 The University reserves the right to restrict remote and mobile working if information risks are not being managed in accordance with this, and other University policies.

5.15 All information security incidents arising from mobile or remote working should be reported to IT Services in line with the **Information Security Controls Policy**.

5.16 If mobile and remote working results in a security incident, associated devices and user accounts may be disabled without notice. Further remote access may be restricted indefinitely to protect University information.

5.17 In accordance with the **Acceptable Use Policy**, organisational mobile devices, must be returned to the University when requested or no longer required.

5.18 A range of technical controls will be implemented by IT Services to ensure that mobile and remote working is in accordance with this policy.

6 Glossary of Terms

6.1 *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[1]. 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. Figure 1, below, defines what is meant by an enterprise asset and provides examples – although it should be noted that this list is not exhaustive.

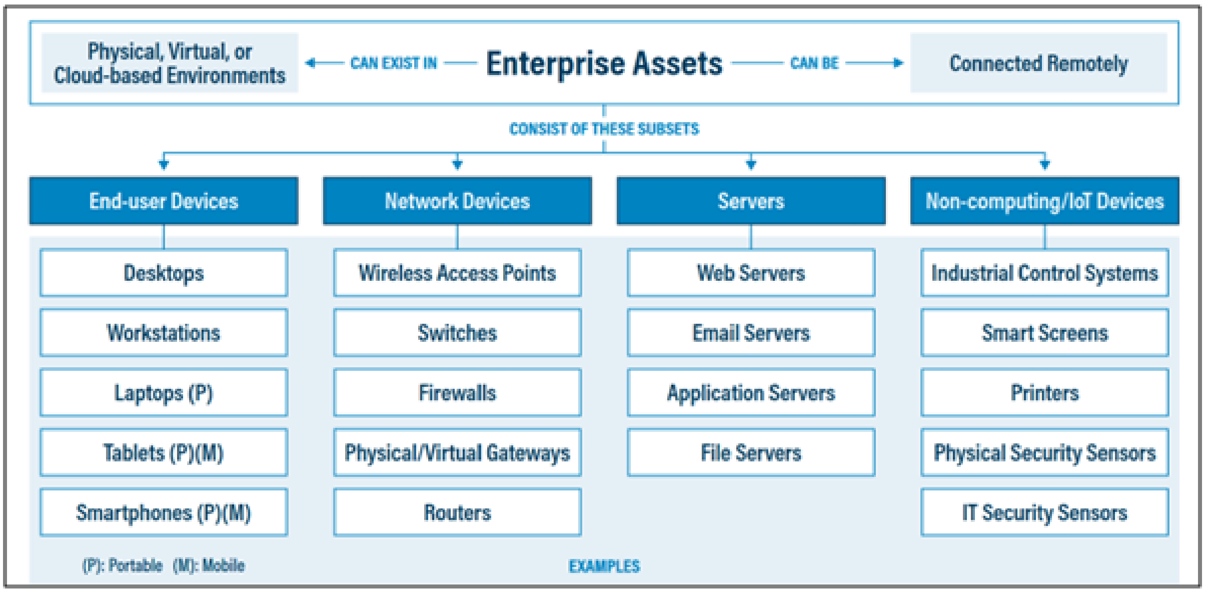

Figure 1: Enterprise Asset definition according to CIS Controls v8

6.2 *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[2] [3]. This balances the usability of BYODs against securing *organisational data* and minimising data breaches.

6.3 *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[4]. Example devices are listed in figure 1, above, specifically those in the End-User Devices column with a (M).

[1] CIS Controls Acceptable Use Policy Template (https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)

[2] https://www.trio.so/blog/mobile-application-management/

[3] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune

[4] https://csrc.nist.gov/glossary/term/mobile_device

6.4 *Mobile Device Management* = Also known as MDM, this is a device-centred management approach[5]. 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[6]. 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.

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

6.6 *Personal 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[7].

[5] https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune

[6] https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management

[7] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/

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

7.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[8]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[9]. A brief definition of each role is given in the table below.

7.2 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
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Executive Director of Infrastructure Services
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

8 Version Control

Version	Author	Date approved	Relevant section(s)
2.0	Dan Chambers, Stewart Doyle	9 November 2021	All
3.0	Hollie Huxstep	02 January 2024	All
4.0	Hollie Felice	08 May 2025	All

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