UNIVERSITY OF HULL

Mobile and Remote Working Policy

Classification:	Policy
Version Number:	2.0
Status:	Approved
Approved by (Board):	University Leadership Team
Approval Date:	9 November 2021
Effective from:	9 November 2021
Next Review Date:	Annual
Document Authors:	Dan Chambers
Document Owner:	Security and Architecture Manager, ICT (Steph Jones)
Department/Contact:	support.hull.ac.uk
Summary:	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
Scope:	This policy applies to all University members and third parties
Collaborative provision:	Not mandatory
Assessment: **(where relevant)**	Not applicable
Consultation: **(where relevant)**	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Governance and Assurance Policy, Data Protection Policy, Information Security Controls Policy and sub-policies
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

All printed versions of this document are classified as uncontrolled.

A controlled version is available from the university website.

Mobile and Remote Working Policy

1. Introduction

1.1. Mobile working and remote access extends 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.

3. Scope

3.1. This policy applies to all University members and all third-parties accessing University systems and information 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 the campus or the campus network.

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 that cannot offer the same level of physical security as University campus locations.

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

4.3. **Loss of credentials**: If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.

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 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 all 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 systems 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 (those designated as Information System Owners should work with the Solicitors Office 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. End user guidance shall be made available for those engaging in mobile and remote working. This will cover approved technologies and acceptable use.

5.5. In order to assure the confidentiality and integrity of University systems and information, only approved technologies may be used for remote access and mobile working.

5.6. 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.

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

5.8. In the event that 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.

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