Information Security - Mobile and Remote Working Policy

A University wide Information Security policy produced for the Information Security Strategic Risk Group.

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-POL-MRW-001
VERSION	1.0
DATED	01 August 2026
DOCUMENT AUTHOR	Cybersecurity Manager
DOCUMENT OWNER	Cybersecurity Manager

Contents

1. Introduction

The University of Strathclyde recognises that mobile and remote working supports flexibility, productivity, and collaboration across teaching, research, and administrative functions. However, working outside of secure University premises presents increased information security risks. This policy sets out the obligations and responsibilities for staff, students, contractors, and third parties when accessing, storing, or processing University digital data on mobile devices.

The objective is to ensure that digital information remains secure, that legal and contractual obligations are met, and that the reputation and operational integrity of the University IT systems are protected.

2. Scope

This policy applies to:

- All staff, students, visitors, contractors, and third parties using University ICT resources.
- All mobile devices which are used to access University data.

3. Risks

3.1 Loss or theft of devices

Devices such as laptops, tablets, and smartphones are inherently portable and therefore at higher risk of being lost or stolen. Without adequate protection (encryption, strong authentication, remote wipe), a lost device could expose sensitive University information.

3.2 Shoulder Surfing

When working in public or shared spaces, screens may be overlooked by unauthorised individuals. This visual disclosure of confidential information can lead to data breaches, reputational harm, or misuse of information.

3.3 Unauthorised access

If devices are not adequately secured with strong passwords, PINs, or multifactor authentication, they may be accessed by unauthorised persons. This includes both malicious actors and unintended users (e.g. family members using a staff laptop at home).

3.4 Tampering

Remote and mobile devices can be tampered with if left unattended, either physically (e.g. insertion of malicious USB devices) or digitally (installation of malware). Such activity can compromise the confidentiality, integrity, or availability of university systems and data.

3.5 Data Leakage

Storing University data on personal devices, consumer cloud services, or removable media outside of approved platforms can increase the risk of loss, unauthorised disclosure, or non-compliance with data protection regulations.

4. Policy

Users who are working remotely, shall:

4.1 Comply with the University's Acceptable Use Policy (AUP) when working remotely. The Acceptable Use Policy is available here.

4.2 Not access, process, display, or discuss confidential, sensitive or personal University information in any location where it may be seen, overheard, recorded, or accessed by unauthorised individuals. This includes public places, shared or uncontrolled environments, public transport, cafés, libraries, conferences and partner premises.

4.3 Ensure that their working environment provides an appropriate level of privacy, including ensuring that screens, documents, and conversations cannot be observed or overheard by unauthorised individuals.

4.4 Users shall take appropriate precautions when using public, free, shared, or otherwise untrusted networks, including Wi-Fi in cafés, hotels, airports, public transport, conferences, libraries, and partner premises.

4.4.1 Users must not ignore browser, certificate, security, or device warnings when accessing University systems or information. Do not connect to the network if you receive warnings.

4.4.2 Where accessing confidential, sensitive, restricted, or personal University information over public or untrusted networks, users must use University-approved secure access methods, such as VPN or other approved security controls from your IT department.

4.5 Report information security incidents, including the loss or theft of devices, to the appropriate University helpdesk or incident reporting channel immediately.

Email – help@strath.ac.uk
Phone – 0141 548 4444

Where personal data may be involved, the Information Governance Unit should also be notified immediately

4.6 University information must only be stored or processed using University-approved systems, services, repositories, or platforms. This includes University-provided services such as OneDrive, SharePoint and Teams, and other systems or external platforms that have been approved for the relevant teaching, research, administrative, partnership, or contractual purpose.

4.6.1 Users must not use personal email accounts, personal cloud storage, consumer file-sharing services, messaging apps, or other unapproved services to store, process, or share University information.

4.6.2 Where University information requires to be stored or processed outside standard University platforms, approval must be obtained before use by Central or Faculty IT, who may engage with Cybersecurity, Information Services and/or Information Governance Unit.

4.7 Use the University VPN when accessing confidential or sensitive information remotely and shall only do so from a University-managed device.

4.7.1 This policy will be reviewed and updated following approval of the University's data classification and sensitivity labelling policy.

4.8 Only perform IT Systems Administration or privileged activities, including the use of accounts with elevated permissions, from university-managed devices.

4.9 Lock their devices when unattended and ensure automatic screen locking is enabled.

4.10 Not allow family members or other unauthorised individuals to use devices that are logged in to university accounts or have access to university systems or data.

4.11 Avoid printing confidential or sensitive information when working remotely. Where printing is necessary, documents must be securely stored and disposed of in accordance with university policy,

4.12 Users must seek advice from the University prior to accessing University systems from locations assessed as high risk by the UK Government/NCSC, particularly where sensitive or restricted information is involved.

5. BYOD (Bring Your Own Device) / Personal Devices

5.1 The University recognises that staff, students, and visitors may use personally owned or unmanaged devices to access University networks and services, including Eduroam and web-based University systems.

5.2 Personal and unmanaged devices may only be used to access University systems and information where the University has permitted such access (e.g. Eduroam and Wireless systems, Email, SharePoint, etc) and where required security controls are in place.

5.3 Personal and unmanaged devices must not be used to:

5.3.1 Perform IT Systems Administration or privileged functions

5.3.2 Access or process highly confidential or restricted information

5.3.3 Store University information locally unless explicitly permitted

5.3.4 Bypass University security controls, including multifactor authentication, conditional access, mobile application management, device compliance checks, or session restrictions.

5.3.5 Connect to the VPN service.

5.4 Users shall ensure that any devices under their control which are used to access University systems or data are appropriately secured, including:

- Authentication:
    - Mobile phones and tablets are protected by a PIN of at least six digits, or equivalent strength, and/or biometric authentication.
    - Laptops are protected by a password which meets the University password complexity and guidance.

- Supported by the device vendor and kept up to date with security patches.
- Encrypted using full disk encryption.
- Running reputable and fully up-to-date anti-malware software on laptops and PCs, where appropriate.

5.5 Access to University systems from personal or unmanaged devices may be subject to additional controls, including multifactor authentication, conditional access restrictions, and session limitations.

5.6 Users must report the loss, theft, compromise, or unauthorised use of any personal or unmanaged device that has been used to access University systems or information.

Email – help@strath.ac.uk
Phone – 0141 548 4444

6. Monitoring

The University may monitor the use of its networks, systems, devices, and services for lawful purposes, including ensuring compliance with university policies, detecting and responding to security threats, maintaining system integrity, and supporting investigations.

Monitoring will be conducted in accordance with applicable UK data protection and privacy legislation, the University's Acceptable Use Policy, relevant Jisc guidance, and other applicable University policies. Monitoring activities will be proportionate, necessary, and subject to appropriate governance and oversight.

7. Non-compliance

Failure to comply with this policy may result in one or more of the following actions, depending on the nature and severity of the non-compliance:

- Restriction or blocking of device access to university systems or services.
- Withdrawal of access to university-managed devices or services.
- Disciplinary action in accordance with the University's disciplinary procedures for staff.
- Action in accordance with relevant contractual, academic, or regulatory processes for students, contractors, or third parties.

8. Supporting Documents

- Information Security Policy
- Jisc JANET AUP
- Legal Framework for ICT
- Acceptable Use Policy
- Mandatory Training Policy
- Data Protection Policy
- Records Management Policy

9. Document Information

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	August 2026	Cybersecurity Manager	First version.
Next Review date			
August 2028			

Distribution

NAME
All users of IT systems.

Approval

NAME	POSITION	GROUP	DATE