v1

Mobile and Remote Working Policy

1. Purpose

1.1 The purpose of this Policy is to ensure that the provision of mobile telephony and data services is aligned with the business needs of the University while preserving the security of our information resources.

2. Introduction

2.1 Mobile and remote working is ingrained in the business activities of the University, enabling the flexible learning, teaching and working practices that many of us take for granted. Central to this practice is the requirement for authorised individuals to access our information resources anywhere and at any time.

2.2 Alongside the significant benefits of mobile and remote working are the accompanying risks and legislative obligations placed on the University to ensure that the confidentiality, integrity and availability of its information resources are protected by appropriate security controls.

2.3 Mobile devices (including laptops, tablets, smartphones, and removable storage devices) are widely used for both personal and professional use, and susceptible to loss by theft, cyber-attack and data leak or loss.

3. Scope

3.1 This policy applies to all staff, students, visitors, contractors (contractors should be sent the policy as part of their engagement) and third-party agents. It includes mobile devices either personally owned or owned by third parties or contractors issued by the University that are used to access the University's data and information resources.

3.2 The policy also covers University information in hard copy format used for remote and mobile working.

3.3 Special Categories or "red" data is defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data used for identification, data concerning health or data concerning a person's sex life or sexual orientation. Special category data, or data relating to criminal offences and convictions, must not be taken off-site without the express permission of the Data Protection Officer or their delegated authority.

3.4 Any exception to this policy must be approved by University Secretary & Information Governance Lead and Data Protection Officer or Chief Information Officer & Chief Technology Officer or their nominee.

4. Links to other policies

4.1 This policy supports the University's Data Protection Policy, the Information Security Policy (under development), the Bring Your Own Device Policy and the Regulations for the Use of Computer Facilities.

5. Principles

5.1 The University will implement appropriate measures to mitigate information security risks associated with its remote and mobile working practices.

5.2 The University will provide user awareness and training, relevant policies and guidelines to promote good security practices for remote and mobile working. It will monitor compliance with policies.

5.3 The University's Data Protection Policy, Data Retention Policy and any data handling procedures must apply when accessing University information resources for all remote and mobile working. The following basic rules must apply:

- Sensitive or highly sensitive University data including personal identifiable data must be accessed and/or shared only on a "need-to-know" basis.
- Data confidentiality, integrity and availability must be maintained at all times in all mobile and remote working situations.

5.4 Securing Mobile Devices

5.4.1 All mobile devices whether personally owned or issued by the University that are used to access or process University data must be protected by a password or pin code*. Where possible, disk encryption should be used.

(*at least a 6-digit pin code must be used but a stronger alphanumeric password of at least 8 characters is recommended.) If the device is not registered with the University's Mobile Device Management service, password requirements will apply to Microsoft 365 applications used with a BSU account instead of at the device level.

5.4.2 University issued mobile devices must be reset to factory settings and pin codes removed before being reissued. This will be undertaken by IT Services to prevent data leakage between users.

5.4.3 Passwords or pin codes on mobile devices that access university IT resources must be kept private. No one else must have access to the device; this includes family members.

5.4.4 Use of University issued mobile devices for personal purposes must be reasonable and minimal and must not be used for activities that could expose the device or University data to information security risks or excessive cost.

5.4.5 Unlicensed software must not be installed on any university issued devices.

5.4.6 “Jailbreaking” - i.e. to remove software restrictions imposed by the manufacturer - changing the security settings or amending configuration files on any mobile device issued by the University is prohibited. This includes disabling passwords, pin codes and any installed security programs (e.g. Anti-Virus or remote management applications). Jail broken or rooted personal devices will be prohibited from accessing University data.

5.4.7 Email links and attachments should be accessed with care as they may contain malware or viruses that could infect mobile devices. Any suspected malware or virus infection relating to a university-issued mobile device must be reported to the IT Service Desk as soon as possible.

5.4.8 Personally owned devices must be adequately protected against the threat of malware, viruses or other compromise. For example, home PCs and laptops must have up-to-date anti-virus software installed, operating systems and applications must be kept up-to-date and patched to remove any known security vulnerabilities.

To ensure this, personally owned devices which the user chooses to use for access to university data must register with the University’s Mobile Device Management (MDM) service to ensure an acceptable level of security is maintained, in line with the University’s Bring Your Own Device Policy.

5.4.9 Mobile devices and laptops must not be kept in full view in a vehicle even for a short period of time but stored away e.g. in the boot of the car. Mobile devices must not be left in a vehicle overnight, even in a locked boot.

5.4.10 During a long absence from a work area or at the end of a workday, mobile devices should be locked away in drawers or cabinets etc. or carried by the user if practicable.

5.4.11 Mobile devices must not be left unattended in public places or an open area in a University building even for a very short period of time.

5.4.12 When travelling by air and subject to the airlines and local regulations and law, mobile devices must always be carried in the cabin and not placed with checked- in items.

5.4.13 All mobile device users must take shared responsibility for the security of University issued mobile devices and the data they may hold.

5.4.14 In the event that a University-owned smart phone is stolen, the user must notify the police, security, their line manager and the IT Service Desk as soon as possible. The University will arrange for the immediate remote removal of University data and a block put on the use of the device.

5.4.15 In the event of a personally owned device being lost that either contains University data or presents a risk to University data, the user must notify the police, security, their line manager and the IT Service Desk as soon as possible. The University may arrange for the immediate remote lock of University data and request that a block put on the use of the device.

5.4.16 Any laptop or other mobile devices issued to staff and the data it holds remain the property of the University and must be returned to the IT Service Desk when leaving the University or when the device is no longer required for work. The device may not be retained.

5.4.17 There are no exceptions to the policy requirement for University staff to return University owned devices when departing from the University. Personal data must be removed from the device before returning it to the University. IT Services do not backup devices returned to them before wiping and re-issuing devices. It remains your responsibility to ensure your personal data has been backed up.

5.5 Securing Data

5.5.1 Any personal data that is taken off-site must be appropriately encrypted, both at rest and in transit.

5.5.2 At all times, appropriate safeguards must be in place to prevent unauthorised access to University data arising from mobile or remote working.

5.5.3 When not in use during mobile and remote working, store confidential papers away in a secure place e.g. locked cabinet or drawer. Device screens must be locked with passwords or pin codes when left unattended. This can easily be done by using the “Windows key” + “L” on a PC and by choosing Lock Screen from the Apple menu (or Command + Control + Q) on an macOS device.

5.5.4 Keep confidential information whether digital or paper-based from public view or access during remote or mobile working.

5.5.5 Store University data on encrypted storage drives such as encrypted USB drives** where the University’s network is not available or on the local drive of a university issued laptop. Any changes made to files (or data) normally stored on university shared drives whilst not connected to the University’s network should be copied back to the normal storage location when the network becomes available, being careful not to overwrite any newer changes.)

(**contact Central Services if you require an encrypted USB drive).

5.5.6 University data (digital and paper based) and IT equipment must be disposed of safely and lawfully in accordance with the University’s Disposal of IT Equipment and Data Retention schedule.

5.5.7 Mobile devices should never hold the sole copy of any important University data.

5.6 **Wi-Fi Connection:** Public or free Wi-Fi should be used with caution during mobile and remote working, and websites visited should be checked to ensure they are genuine. Confidential data (including login details and other business sensitive information) must not be transmitted or accessed on a non-secure Wi-Fi (e.g. over the unencrypted http web protocol) as it is possible that the information could be viewed by unauthorised individuals.

5.7 **Remote Access:** Secure remote access or VPN connections provided by the University must be used to access network shared areas, and other information systems that may hold sensitive data. This includes remote access by system administrators. If you are any doubt as to the security implications of your remote work, contact the IT Service Desk an always err on the side of caution.

5.8 **Email and Cloud Solutions**: Only University provided or approved email and cloud facilities must be used for remote and mobile working – currently making use of the University's Microsoft Office 365 subscription. Personal email and cloud solutions (including other Office 365 accounts) must not be used for the University's business.

5.9 The University reserves the right to refuse network connections for particular devices or software where it considers that there is a security or other risk to its data or information resources.

5.10 The University owns all information resources, and all data present, transmitted or processed on a mobile device during the University's business or otherwise on the University's behalf – irrespective of who owns the mobile device.

5.11 It may on occasion be necessary for the University to request access to a personally owned mobile device, such as in the case of a security breach. Every effort will be made to ensure that the University does not access private information relating to the individual. If a user is unhappy with this clause they should not use their personal device to access or process University data.

6. Compliance

6.1 All staff, researchers, third party agents and visitors must take responsibility for ensuring the security of the information they handle during remote and mobile working.

6.2 Loss of University data caused by disregarding this policy will be the sole responsibility of the user of the mobile device, and the appropriate disciplinary action may follow. Reporting losses or suspected losses quickly will help the University take action to protect the data and meet its compliance obligations.

Prompt reporting will be considered as a mitigation in the event of disciplinary action being taken.

Document Details

Responsible Office: IT Services

Responsible Officer: Chief Information Officer

Approving Authority: Senior Leadership Group

Date of latest approval: 15 April 2024

Effective Date: 15 April 2024

Related Policies and Procedures: Endpoint Device Purchasing, Deployment and Management Policy

BYOD Policy

Mobile and Remote Working Policy

Regulations for the use of computer facilities

Supersedes: (new)

Next review due: April 2026