UNIVERSITY OF
WEST LONDON
The Career University

Mobile and Remote Working and Mobile Device Policy

Responsibility of: IT Services
Approval Date: May 2018
Review Date: May 2020
Approved By: IT Steering Group (ISG)

1. Introduction

1.1. Mobile and remote working is essential for and enables flexible learning and working practices. The need for access to the University's information resources on and off-site makes it necessary to maintain availability to these resources anywhere and anytime to authorised individuals.

1.2. As much as mobile and remote working provides great benefits, it is necessary to balance these benefits against the risks they may present by ensuring appropriate security controls are in place to maintain the confidentiality, integrity and availability of the University's information resources in mobile and remote working situations.

1.3. Mobile devices (Laptops, tablets, smart phones and removable storage devices) are highly desirable and widely used for personal purposes and for mobile and remote working. As a result, they are susceptible to loss or theft, cyber hacking, and data leak or loss.

1.4. Staff should avoid the transport of personal data in any form - by email, in hard copy, on an electronic device or memory stick

2. Objective

2.1 This policy is to ensure that the security of the University's data and information resources are maintained in mobile and remote working situations.

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 and 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 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 his/her delegated authority.

3.4 Any exception to this policy must be approved by University Secretary & Chief Compliance Officer or Associate Pro-Vice Chancellor & Chief Information Officer or his or her nominee, using the exception form attached in Appendix 1 (under development).

4. Links to other policies and procedures

4.1. This policy supports and is referenced in the University's Data Protection Policy, the Information Security Policy and the Acceptable Use of Information Assets Policy (copies of which can be found here https://www.uwl.ac.uk/about-us/policies-and-regulations).

4.2. This policy also supports the University's Occupational Health, Safety and Welfare Policy (copy of which can be found here https://www.uwl.ac.uk/sites/default/files/Departments/About-us/Web/PDF/health_and_safety_policy_january_2017_1.pdf)

5. Principles

5.1. The University will implement as 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, procedures and guidelines to promote good security practices for remote and mobile working and 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.)

5.4.2. University issued mobile devices must be reset to factory settings and pin codes removed prior to returning the devices to IT Services when no longer required.

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” - that is 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 personal devices must not be used to access 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’s 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, virus 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.

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 work day, mobile devices should be locked away in drawers or cabinets etc. or carried along 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 airline’s 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 removal 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 appropriate line manager or 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 and apps must be removed from the device before returning it to the University.

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 Sleep from the Apple menu (or “Ctrl” + “Shift” + “Media Eject/Power”) on an Apple Mac computer.

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 the IT Service Desk 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. Exchange ActiveSync: Passcodes with a minimum length of 6 digits must be enabled on any mobile device that is activated to use the University's Exchange ActiveSync.

5.10. 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.

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

5.12. The University reserves the right to request access to inspect, or delete University data held on a personally owned mobile device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the University does not access private information relating to the individual. If a user is are unhappy with this clause then they should not use their own 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 in line with the University's information security and data protection policies.

6.2. Students must ensure that the use of their mobile devices to access the University's information resources must not involve activities that could expose these resources to information security risks. Advice and training will be provided during the IT induction and periodically through the academic year.

6.3. 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 as soon as possible will help the University to take action to protect the data and meet its compliance obligations. Prompt reporting will be considered as a mitigation in any disciplinary action taken.

7. Relationship with other policies

7.1. This Policy is related to the following University policies:

- Information Security Policy and its supporting policies
- Data Protection Policy
- Acceptable Use of Information Assets Policy
- Occupational Health, Safety and Welfare Policy
- Data Retention Schedule
- Disposal of IT Equipment Policy

8. Policy Review and Maintenance

8.1. This policy will be reviewed and updated annually to ensure that it remains appropriate in the light of changes to business requirements, statutory laws or contractual obligations.

Acknowledgements

UWL gratefully acknowledges the University of Greenwich Information and Library Services upon whom policy this document is based.

9. Appendix and Links

9.1. Appendix A: Do's and Don'ts for Mobile Devices

9.2. University information security policies (https://www.uwl.ac.uk/about-us/policies-and-regulations)

9.3. University Data Protection Policy (https://www.uwl.ac.uk/about-us/policies-and-regulations/privacy-and-data-protection)

9.4. University Health and Safety Policy, including requirements for working remotely safely (DSE self-assessment questionnaire - https://safety.uwl.ac.uk)

Appendix A – Guidance for good mobile and remoting working practice and protecting mobile devices

Dos and Don'ts

- Do create and use a password or pin code to prevent unauthorised access to your mobile device.
- Do turn your mobile device off or use screen lock and put it in an appropriate carrying case when travelling.
- Do keep all drinks and any other liquids away from your mobile device. Any spillage on the device can result in data loss and expensive repairs.
- Do avoid turning off your laptop when the hard disk light is on. This can result in data corruption and / or data loss.
- Do make sure that you always copy back any amended documents or data to your departmental shared folder after working remotely, making sure you do not overwrite newer data.
- Do report a loss or theft as soon as possible.
- Be aware of your surroundings and ensure no-one can "shoulder-surf" your password or see the data on your screen.
- Do use antivirus/malware software to check and remove virus or malware on your mobile device if you suspect it may be infected with a virus or malware.
- Do inform the IT Service Desk immediately if you believe a University device is infected with a virus/malware or has been compromised.
- Don't leave your mobile device unattended. If you need to leave your desk, put the device in a lockable drawer or take it with you. Lock your office door if appropriate. If you are travelling and cannot keep your mobile device with you when it is not in use, then where possible, store the device in a safe, or at the very least lock it in your room.
  Don't use your mobile device to access sensitive University data in public places if there is a possibility that the data could be breached.
- Don't "jailbreak" your mobile phone.
- To encrypt a file, first choose a good password, for example by choosing three random words and putting them together. Then you can either:
  - Encrypt a Word or Excel file from the application by choosing File, Protect Document, Encrypt with password. You will need the document to be in the newer .docx or .xlsx formats.
  - Right-click any file, choose 7-Zip, Add to Archive, make sure the encryption method is set to AES-256, and enter the password.
  - Remember not to store or transmit the password together with the encrypted file.