UNIVERSITY of GREENWICH

Document Reference Number	UoG/ILS/IS 009
Date	January 2021
Title	Policy for Mobile and Remote Working
Owning Department	Information and Library Services
Version	5.0
Approval Date	29/01/2021
Review Date	28/01/2022
Approving Body	Information Assurance and Security Committee

Policy for Mobile and Remote Working

1.0 Introduction

1.1 Mobile and remote working enables flexible learning and working practices, necessitating the use of mobile devices and the availability of information resources when required.

1.2 Mobile and remote working has its benefits and risks. It is essential to balance these opportunities and risks to ensure the confidentiality, integrity and availability of the University's information resources are maintained in mobile and remote working situations.

1.3 Mobile devices (such as laptops, tablets, phones and removable storage devices) are highly desirable and widely used to support flexible working. As a result, they are susceptible to loss, theft, hacking, data leak or loss.

2.0 Objective

2.1 This policy sets out the expected practices to safeguard the University's information resources and IT assets in mobile and remote working situations.

3.0 Scope

3.1 This policy applies to all members of staff, students, researchers and third parties working in partnership with the University. It applies to the use of personally owned and University issued devices that access and process University information.

3.2 The policy also covers the use of University information in hard copy format during mobile and remote working.

4.0 Reference to International Organisation for Standardisation (ISO) 27001

4.1 This policy complies with the University's Information Security Strategy and draws upon the ISO 27002 Code of Practice.

5.0 Requirements

5.1 The University's Data Classification, and Information Labelling and Handling Procedures and the Data Protection Codes of Practice must be adhered to when accessing University information resources for all mobile and remote working.

5.2 Approval must be obtained from line managers and/or Faculty Operating Officers if a device that has been funded by a research project can leave with a staff member at the end of employment (University data and licensed software must be wiped off the device).

5.3 **Securing Devices**

5.3.1 **All Devices**

5.3.1.1 Devices whether personally owned or issued by the University that access or process University information must be protected using the security features of the device e.g. biometrics, pin code or password. Where possible, disk encryption should be used.

5.3.1.2 Passwords or pin codes on devices that access University information resources must be kept private.

5.3.1.3 Devices must have active and up-to-date antivirus protection and use device encryption where the device features such services.

5.3.1.4 Email links and attachments should be accessed with care as they may contain malware or viruses that could infect devices.

5.3.2 **University Issued Devices**

5.3.2.1 University laptops must have the University asset management client and endpoint antivirus software installed. Other issued University devices must be recorded in an asset register and must have up-to-date software versions installed. Where possible, these devices should have asset tags.

5.3.2.2 When a University issued device is no longer required, it must be reset to factory settings and the pin code removed before returning it to your line manager or the IT Service Desk.

5.3.2.3 The use of University issued devices for personal purposes must be reasonable and minimal and must not be used for activities that could expose the device or University information to security risks.

5.3.2.4 Unlicensed software must not be installed on any University issued device. The official stores for app download such as App Store, Google Play, and Blackberry must be used for downloading apps. Members of staff requiring specific University licensed software should refer to the Application Management Process and complete the AMP form.

5.3.2.5 "Jailbreaking" is to remove software restrictions imposed by the manufacturer. Changing the security settings or amending configuration files on any University issued device is prohibited. This includes disabling passwords, pin codes and any installed security programs (e.g. antivirus software).

5.3.2.6 Any suspected malware or virus infection relating to a University issued device must be reported to the IT Service Desk as soon as possible.

5.3.2.7 Laptops must not be kept in full view in a vehicle even for a short time, but stored away e.g. in the boot of the car. Devices must not be left in a vehicle over-night, even in a locked boot.

5.3.2.8 During long absences from office desks or at the end of a workday, devices should be locked away in drawers or cabinets, etc. or carried along by the user if practicable.

5.3.2.9 Devices must not be left unattended in public places or an open area in a University building even for a very short period.

5.3.2.10 When travelling by air and subject to the airline's and local regulations and law, devices should always be carried in the cabin and not placed with checked-in items.

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

5.3.2.12 If a University device is stolen, the user must notify their line manager, the IT Service Desk, and the police, as soon as possible. If the loss or theft occurs outside of normal IT Service Desk operating hours, a report must be made on the next working day following the event.

5.3.2.13 If a smartphone is lost or stolen, the incident must be reported to the IT Service Desk as soon as possible to minimise the potential costs associated with any misuse. Garnell, the network service provider will block the number and a new handset can be arranged by the relevant department with Garnell by contacting the ILS Network Operations Team.

5.3.2.14 IPads, tablets and smartphones used for work purposes must have remote data wipe off enabled and where device lockout or deactivation functionality exits, this should also be enabled.

5.3.2.15 Any laptop or other devices issued to staff and the data it holds remain the property of the University of Greenwich 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 cannot be retained.

5.3.2.16 Only section 5.2 will apply to any exception to the policy for University staff to return University issued devices when departing from the University. Personal data and apps must be removed from the device before returning it to the University. If required, specific University licensed software may need to be removed before the device is reassigned.

5.3.3 **Personal Devices**

5.3.3.1 Personal devices used for work purposes must have up-to-date software versions to mitigate software vulnerabilities that could compromise the data on the devices.

5.3.3.2 All University information stored on a personal device must be deleted.

5.3.3.3 University applications (e.g. Multifactor authentication, Outlook, Teams) on personal devices must be deleted when the device is no longer used.

5.3.3.4 A factory reset should be completed on the device before it is sold, transferred, exchanged or disposed of. The line manager has to ensure devices are reset before the user leaves the University.

5.3.3.5 The University will not monitor the content of personal devices. However, the University reserves the right to monitor and log data traffic transferred between such devices and University systems, both over internal networks and connecting to the University's network via the Internet.

5.3.3.6 All work-related, online activities must be carried out in line with the University's Information Security Policies. This requirement applies equally to personal devices.

5.3.3.7 Access to certain services from personal devices, such as Office 365 applications can result in the ability for the University to remove or wipe either an entire device or corporate content associated with the applications.

5.3.3.7.1 This may take place where there is a major security concern or incident that requires the need to wipe data off the device to minimise any associated risks.

5.3.3.7.2 Consent will be requested from the device owner where the entire device might be wiped during the process however the University reserves the right to wipe work-related data without consent.

5.3.3.8 For email, Microsoft Outlook client should be used. For mobile devices including IOS and Android, Outlook is available from the relevant app store. For PC and Mac devices, Outlook is available as part of the Office 365 application suite.

5.4 Securing Data

5.4.1 University information must be transferred from a mobile device to the appropriate shared drive, Teams or OneDrive area at the earliest possible time and deleted from the device. Data must be deleted immediately from the device if required by the University to do so.

5.4.2 At all times, appropriate safeguards must be in place to prevent unauthorised access to University information during mobile and remote working.

5.4.3 In mobile and remote working situations, store confidential papers away in a secure place e.g. locked cabinet or drawer when not in use. Device monitors must be locked when unattended.

5.4.4 Keep confidential information whether digital or paper from public view or access.

5.4.5 Store University information on University network drives or M365 environment. Where these storage areas are not available, store University information on an encrypted drive such as an encrypted laptop or USB drive. Any changes made to files (or data) stored on an encrypted laptop or USB drive whilst the University's shared drive or M365 is not available, should be copied back to its primary location when they become available.

5.4.6 University information and IT equipment must be disposed of following the University's Policy and Procedure for Disposal of IT Equipment and Code of Practice for Retention and Disposal of Records and Data.

5.4.7 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 an unsecured WI-FI as it may be possible that the information could be viewed by unauthorised individuals.

5.4.8 Remote Access: Secure remote desktop access or VPN (virtual private network) solutions provided by the University must be used to access the network shared areas and other information systems that may hold sensitive data.

5.4.9 Multifactor authentication (MFA) is the use of additional identifiers e.g. pin codes to verify users. MFA is required for remote access to internal information resources and all members of staff are required to register their devices (personally owned or University issued) for MFA to enable access to these resources.

5.4.10 Cloud facilities: Only University-approved cloud facilities must be used for mobile working to comply with the University's Policy for Data Classification, Information Labelling and Handling Procedures. Personal email and cloud solutions must not be used for the University's business.

5.4.11 The University reserves the right to refuse network connections for some devices or software where it considers that there are security risks to its information resources or IT assets.

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

5.4.13 The University reserves the right to request access to inspect or delete University information held on a personally owned 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.

6.0 Compliance

6.1 All staff, students, researchers and third parties must take responsibility for ensuring the security of the information they handle during mobile and remote working in line with the University's Information Security and Information Compliance Policies.

6.2 Students must ensure that the use of their devices to access the University's network resources must not involve activities that could expose these resources to information security risks.

6.3 Loss of University information caused by disregarding this policy will be the responsibility of the user of the device, and the appropriate disciplinary action will follow.

7.0 Exception

7.1 Any exception to this policy will be reviewed and approved by the Director of Information and Library Services or a nominee.

8.0 Related Policies

- Information Security Policies
- Information Compliance Policies
- Risk Management Policy and Guide

9.0 Policy Review and Maintenance

9.1 This policy will be reviewed annually.

10.0 Appendix A

10.1 **Good Practice Guidance for Mobile Working and Protecting Mobile Devices**

- Use a password or pin code to prevent unauthorised access to your device.
- Turn your device off or use screen lock and put it in an appropriate carrying case when travelling.
- Keep all drinks and any other liquids away from your device. Any spillage on the device could result in data loss and expensive repairs.
- Avoid turning off your laptop when the hard disk light is on. This can result in data corruption and/or data loss.
- Ensure you always copy back any amended documents or data to your departmental shared area after working remotely.
- Report a loss or theft of your device as soon as possible.
- Use Privacy Filter if working in a public place (e.g. on a train, airplane or in a hotel lobby).
- Use antivirus/antimalware software to check and remove viruses or malware on your device if you suspect it may be infected with a virus or malware.
- Inform the IT Service Desk immediately if you believe a University device is infected with virus/malware or has been compromised.
- Keep the device away from high temperatures and hazardous environments (i.e. don't use or store near radiators or fan heaters). Mobile devices are designed to work within a defined temperature range so exposing them to extreme temperatures (highs or lows) may cause the device to malfunction or behave unpredictably. Avoid using laptops in temperatures over 50°C.
- Your device should not be left unattended in public areas or for a prolonged absence in an open-plan office. Lock it away or take it with you. Lock your office door if appropriate. If you are travelling and cannot keep your device with you when it is not

in use, where possible, store the device in a safe, or at the very least lock it in your room.

- Use your device to access only non-sensitive/non-confidential information in public places if there is a possibility that the information could be breached.
- **Don't** "jailbreak" your mobile phone.