Loughborough University

Information Security

Mobile & Remote Working Policy

Version 1.2:
Approved November 2021
Updated March 2022
Review March 2025

Mobile & Remote Working Policy

1. Policy Overview

This policy sets out the expected working practices and safeguards to be followed by individuals when working remotely and away on one of the University campuses. It covers the use of both University owned devices and personally owned devices for remote working and recognises that such working may take place elsewhere in the UK or internationally including at the individual's home address.

2. Policy Audience

This policy applies to all members of staff and including post-graduate researchers. It also represents the practice expected of third-party individuals working in partnership with the University who have access to university owned information and who are accessing that information away from a secure environment on one of the University's campuses.

3. Policy Scope

Staff may be working remotely in line with the University's policies, and where arrangements have been agreed with their line manager.

Both University and personally owned devices may be used for remote working and information security risks will need to be considered carefully in the context of the University's information security policies depending on the nature of the information to be accessed, the device(s) to be used and the nature of the remote environment.

4. Use of Personally Owned Devices

The University recognises the benefits brought by use of personally owned devices and equipment. They facilitate legitimate working from home and help individuals to manage varied workloads wherever they are located on or off campus. Examples of such devices include:

- Desktop computers (typically at home)
- Laptops
- Tablet computers
- Smart Phones
- Smart Watches

5. Use of Personally Owned Devices in countries that prohibit use of encrypted devices

You should not take encrypted devices into countries that prohibit use of such equipment. Speak to IT Services to discuss your options.

6. Responsibilities of all Staff and Post Graduate Researcher's when using Personally Owned Devices – Set Up of Device

If you use your own device to access University information or to conduct activities related to your role within the University, you must:

- Ensure that you adhere, at all times, to the Acceptable Use Policy;
- Familiarise yourself thoroughly with the device and its security features so you are able to ensure the safety of University information (as well as your own), IT Security Tips;
- Ensure you have a mobile device set up correctly so you can verify your identity by participating in multi factor authentication. Where a mobile device is not available ensure that you have access to a hardware security token;
- Ensure that separate accounts are used on devices shared with family members and any unused accounts are deleted or no longer active (cannot be used to log in). Details for accounts used to access University information and/or systems must only be known by the University employee:
- Ensure that all relevant security and anti-virus features, including anti-virus and software firewall, are enabled, where appropriate. Anti-virus software must be set to update daily;
- Maintain the device yourself ensuring the Operating System (OS – e.g. Windows, macOS, iOS, Android), Firmware (the software which controls all the components within a device), and additional software (including Apps) are regularly patched and updated. Ensure all security updates for the OS, Firmware and any additional software are installed within 14 days of release. Where possible set software to update automatically. Regularly review and remove or disable any unused software. Unsupported software (software which no longer receives updates or security fixes from the software provider) needs to be either removed from devices or updated to a supported version;
- Ensure operating systems on smartphones and tablets are untampered with i.e. neither rooted or jailbroken (modified or remove or reduce manufacture-imposed security restrictions);
- Set appropriate passwords, passcodes, passkeys or biometric equivalents known only by the account holder. These must be of sufficient length and complexity for the particular type of device, which will be enforced by appropriate IT Systems, and must be changed if shared with others or otherwise compromised;
- Devices must be encrypted where possible; modern smart phones and tablet devices are encrypted automatically by setting a four-digit PIN;
- Take responsibility for any software that is downloaded onto the device. Ensure software is only downloaded from known sources and authorised app stores (App Store and Google Play). All software must be appropriately licensed;
- Set up location tracking services and remote wipe facilities where available. Depending on how your device has been configured, central IT Services may be

able to issue a remote wipe which will enforce the option to erase at least the email content;

- Ensure that Highly Confidential and Confidential information is not stored on the device or personal cloud storage services, this must be stored on the University network or within Microsoft365 such as OneDrive or Teams, and in accordance with the University retention rules;
- If a data breach has occurred (an individual has lost control of University information), this needs to be reported to immediately using the Report a data breach form;
- If Highly Confidential or Confidential information is at risk report any loss or theft of the device to IT Services and implement a remote wipe, if possible;
- Ensure that when a personally owned device is disposed of, sold, or transferred to a third party all University information is securely and completely deleted from it by following the procedures which IT Services, Service Desk should provide;
- For disposal of all University owned devices, please ensure that all WEEE guidelines are followed (note: separate procedures for laptops and for mobile phones

Details of how to access University IT facilities such as email through your own device will be found on IT Services webpages.

The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from any support and advice provided.

7. Working Practices

This section is applicable to use of information from university and personally owned devices and some clauses are also relevant to hardcopy information.

When working away from campus, and when available, the use of the international eduroam wireless service should be used for security reasons and to avoid additional expensive wireless and mobile roaming costs. Further details are available at: https://www.lboro.ac.uk/services/it/staff/network/eduroam/

The majority of wireless networks, including those in coffee shops and hotels, are shared and therefore malicious people can view some of the activity happening on your device. It is therefore essential to use the University Off Campus VPN working on Confidential or Highly Confidential University information, and it is recommended as standard practice. Further details on using the VPN service are available:

You should not use devices owned by third parties to access or process University information (e.g. Internet Cafes) unless these third parties are trusted partners whose relationship with the University is covered by a formal agreement e.g. research partners).

As you would when you are working on campus at your normal work location, when working on a mobile basis you should always ensure that unauthorised individuals cannot access your University IT account, see or access Highly Confidential or Confidential University information (as defined in the Information Categories and Controls Policy).

You must take all reasonable steps to:

- Prevent the theft or loss of information, or unauthorised access to confidential information. Your device should always be locked when not in use or you need to move away from your work area. When not using your device for a long period of time (overnight), turn your device off;
- Ensure that no unauthorised access to Highly Confidential or Confidential information can take place, and follow the University's Data Protection and Information Governance Policies, as well as any commercial agreements which may relate to the information you are accessing or processing;
- Maintain the integrity and availability of information, where possible work on information directly stored within OneDrive or Teams. If required ensure that relevant information is copied back to central University information systems or Microsoft 365 (OneDrive/Teams) where appropriate;
- Ensure that Highly Confidential or Confidential information is not retained on the device for longer than is necessary.
- Report any personal data breaches immediately via the Breach reporting form in accordance with the Information Security Incident Handling Policy.
- Report any security breach immediately to IT Service desk in accordance with the Information Security Incident Handling Policy.
- Ensure University devices or confidential information is not left where it would attract the interest of an opportunist thief. In the home it should be located out of sight of casual visitors and when not in use, it is recommended that it is stored in a locked or sealed environment.

8. Monitoring and Access

The University will not monitor the data content of your personal devices unless the data is stored or synchronised with university systems (email, Microsoft365, OneDrive, Teams etc), however, in certain circumstances, the University has the right to monitor the security posture (status and quality of security features and protections) – of devices accessing University information and log data traffic transferred between your device and University systems, both over internal networks, VPN connections and entering the University via the Internet.

The University also reserves the right to:

- Prevent access from a particular device from either VPN, wired or wireless networks;
- Prevent access to a particular system;
- Enforce a minimum standard for devices which access University information or systems;
- Disable user accounts if deemed to have been compromised or abused;
- Take all necessary and appropriate steps to retrieve information owned by the University.

From time to time, the University may require that you install or update University-approved device management software on your own device.

9. Information Sharing

Please see the Information Sharing policy for guidance on the use of , Cloud Services and third party facilities for collaborative working and information sharing with external partners. Consideration must also be given to the confidentiality or sensitivity of the information you need to share. Please refer to the Information Categories and Control Policy.

10. Loss, Theft or Damage of Device

If a device is damaged, lost or stolen that holds Highly Confidential or Confidential information belonging to the University, this should be reported to the IT Service Desk immediately, regardless of whether the device is University or personally owned. Staff should make all possible enquiries to attempt to locate lost or stolen devices and report any potentially criminal activity to the appropriate authorities.

In the event that a personally owned device is used to access or share University owned information, then the University reserves the right to remotely wipe the device in the event that it becomes damaged, lost or the University becomes concerned that the security of the information has been compromised.