

Mobile Working Guidance

Overview

This document sets out the recommended working practices and safeguards to be followed by staff when working ‘on the move’.  It covers the use of both UR-owned and personal devices for mobile working and recognises that such working may take place on campus, but away from the individual’s main base, or away from these secure environments, either at home or elsewhere in the UK or internationally.

Home Working

Staff may be permitted to work at home in line with the University’s Home Working Guidance and specific arrangements should be agreed with their line manager. Both UR and personally owned devices may be used for home 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 home environment.

In the rest of this policy the term mobile working is taken to include home working.

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

Travelling Internationally with your device

Please note that some countries may have restrictions in place regarding your device and data. E.g., you should not take encrypted devices into countries that prohibit use of such equipment unless you are happy to unencrypt the device. For UR devices, contact the Service Desk for assistance.

Responsibilities 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 should:

* Ensure that you adhere, at all times, to the [Acceptable Use Policy](https://portal.roehampton.ac.uk/information/it/Pages/IT-Policies.aspx%22%20/).
* Familiarise yourself thoroughly with the device and its security features so you can ensure the safety of UR information (as well as your own)
* Ensure that separate accounts are used on devices shared with family members.  Where this is not possible, where available, use with additional security settings within work-related applications (e.g.  Outlook for mobile allows to set an additional passcode etc.)
* Ensure that all relevant security and anti-virus features are enabled, where appropriate (e.g. auto-lock/screen-lock feature after inactivity for more than a few minutes, use separate account with local admin privileges etc.)
* Maintain the device yourself ensuring both the Operating System and additional software (Apps) are regularly patched and upgraded.
* Set appropriate passwords, passcodes (ideally 6 digit), passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device and may be enforced by appropriate IT Systems.
* Devices should be encrypted where possible (note that Apple mobile devices are encrypted automatically if at least the 4-digit PIN is enabled);
* Take responsibility for any software that is downloaded onto the device.
* Set up location tracking services and remote wipe facilities where available until central IT services are available which will enforce the option to erase at least the UR email content.
* Ensure that confidential information is not retained on the device for longer than is necessary.  For UR data always use the supplied one Drive for Business cloud storage
* If UR confidential information is at risk, report any loss or theft of the device to the Service Desk 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 personal and University information is securely and completely deleted from it.  Service Desk can provide advice if needed.

See also [Standard Configuration Details for Computers and other network devices](https://www.roehampton.ac.uk/globalassets/documents/corporate-information/policies/cyber-security-policies/standard-configuration-details-for-computers-and-other-network-devices-.pdf) for details of how UR-owned devices are set up.

Details of how to access University IT facilities such as email through your own device will be found on below:

[Set up the Office app and Outlook on iOS devices - Office Support (microsoft.com)](https://support.microsoft.com/en-us/office/set-up-the-office-app-and-outlook-on-ios-devices-0402b37e-49c4-4419-a030-f34c2013041f)

[Set up email in the Outlook for Android app - Office Support (microsoft.com)](https://support.microsoft.com/en-gb/office/set-up-email-in-the-outlook-for-android-app-886db551-8dfa-4fd5-b835-f8e532091872)

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.

Working Practices

This section is applicable to use of information from UR and personally owned devices, and some advice is also relevant to hardcopy information. When working away from campus, and when available, the use of the international eduroam Wi-Fi service should be used for security reasons and to avoid additional expensive wireless and mobile roaming costs. Further details are available at:

[eduroam | University of Roehampton](https://www.roehampton.ac.uk/Services/IT-and-Media-Services/eduroam/)

[The](http://www.lboro.ac.uk/services/it/out/eduroam/%20%20The) 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 [URApps portal](https://urapps.roehampton.ac.uk/RDWeb/Pages/en-GB/Default.aspx%22%20%5Ct%20%22_blank) or the [UR O365 application suite](https://www.office.com/?auth=2&home=1) (including SharePoint, OneDrive etc.) when working on UR data, and this is recommended as standard practice.

You should not use devices owned by third parties to access or process UR 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. Partnerships, research partners).

Regardless of whether you are working from campus or on a mobile basis you should always ensure that unauthorised individuals cannot see or access UR information. You must take all reasonable steps to:

* Prevent the theft or loss of the device or information.
* Ensure that no unauthorised access to UR information can take place, paying due regard to the provisions of appropriate [UR Polices](https://www.roehampton.ac.uk/corporate-information/policies/) regarding the Data Protection Act and the UR Data Protection Policies as well as any commercial agreements which may relate to the information you are accessing or processing.
* Maintain the integrity of information, by working on relevant information in-situ on UR systems (this ensures it is backed-up) or copy it back to central UR information systems where appropriate.
* Ensure that no UR information is left on any personal device indefinitely (see above).
* Report any security breach immediately to the Service Desk in accordance with the [Data Breach Procedure](https://www.roehampton.ac.uk/corporate-information/policies/).
* Devices must not be used to Store or transmit illicit materials, harass others or engage in outside business while on Campus or being connected to university services.
* Never use your device while driving, operating machinery or carrying out hazardous tasks such as working at height.

Monitoring and Access

UR will not monitor the data content of your personal devices unless the data is stored or synchronised with UR systems (email, workspaces etc), however UR has the right to monitor and log data traffic transferred between your device and University systems, both over internal networks and entering the University via the Internet. The University also reserves the right to:

* Prevent access from a particular device from either wired or wireless networks or both.
* Prevent access to a particular system.
* Disable user accounts if deemed to have been compromised.
* Take all necessary and appropriate steps to retrieve information owned by the University.
* From time to time, UR may require that you install or update UR-approved device management software on your own device.

Loss, Theft or Damage of Device

If a device is damaged, lost or stolen that holds information belonging to the University, this should be reported a.s.a.p. to the Service Desk, 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.

If a personally owned device is used to access or share UR 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.