University of Bristol
Information Security Policy - Mobile and Remote Working

Title	Mobile and Remote Working
Reference	ISP-14
Status	Approved
Version	2.0
Date created	June 2013
Last reviewed	July 2023
Next review	July 2024
Classification	Public

Contents

1. Introduction

This Mobile and Remote Working Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices not located on University premises when devices are used to access University data.

While recognising the benefits to the University (and its members) of permitting the use of mobile devices and working away from the office, the University also needs to consider the unique information security challenges and risks that will necessarily result from adopting these permissive approaches. In particular, the University must ensure that any processing of personal data remains compliant with UK Data Protection legislation.

2. Scope

This policy applies to all members of the University and covers all mobile computing devices whether personally owned, supplied by the University or provided by a third-party. Personally owned, University owned or third-party provided non-mobile computers (for example desktops) used outside of University premises are also within scope.

2.1 Definitions

A mobile computing device is defined to be a portable computing or telecommunications device that can be used to store or process information. Examples include laptops, netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards, wearable devices and smart devices.

University data is classified as any data belonging to the University. This includes emails, office documents, database data, personal and financial data. Data obtained from third parties, including research and clinical data obtained under a data sharing agreement with the University, would also be considered University data.

3. Policy

3.1 Personally Owned Devices

Whilst the University does not require its staff or postgraduate researchers to use their own personal devices for work purposes, it is recognised that there are instances where some University members prefer to use their personal devices. Users must always give due consideration to the risks of using personal devices to access University data and in particular, information classified as Confidential or above according to the University's Information Classification Scheme.

The use of personally owned devices is only permitted subject to the following **minimum security configuration requirements**, and access to University systems may be restricted if these are not met:

- Devices must run a supported version of its Operating System (OS) and must also have the latest security update installed, both for the OS and any installed applications. A supported version is defined to be one for which security updates continue to be produced and made available to the device.

- University data stored or processed on mobile devices must be encrypted.

- An appropriate passcode or password aligned with the University's password guidance, must be set for all accounts which give access to the devices. The use of biometric authentication methods is also acceptable.

- A password protected screen saver/screen lock must be configured.

- Devices that are capable must run Anti-Virus software.

- Software firewalls must not be disabled or updates postponed.

- Do not undermine the security of the device (for example by “jail breaking” or “rooting” a smartphone).

- Devices must be configured to “auto-lock” after a period of inactivity (no more than 15 minutes).

- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.

In addition to the minimum security configuration requirements above, the following **secure behaviours** are required:

- Use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to University data classified as Confidential or above.

- Personally owned devices must not be used for activities that require administrative access. For more detail see Access Control section in System Management Policy (ISP-11).

- Minimise the amount of University data stored locally on the device and do not store any data classified as Confidential or above.

- Access University information assets via the University’s remote access services wherever possible rather than transferring the information directly to a device. See page for more information on remote access: https://uob.sharepoint.com/sites/itservices/SitePages/remote-access.aspx.

- Consider switching on device tracking/location services in the event of device theft or loss.

- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.

- Devices must be disposed of securely, including the removal of University data before disposal, in accordance with the Disposal of Information section of the Information Handling Policy (ISP-07).

3.2 University Owned Devices

The University provided computing devices may be used for remote working. These devices are appropriately configured to ensure that they are as effectively managed as devices that remain within the office environment and meet the minimum security configuration requirements listed above for personally owned devices.

When using University owned devices, the following are required:

- Non-members of the University (including family and friends) must not make any use of the supplied devices.
- No unauthorised changes may be made to the supplied devices.
- Devices assigned to a specific user should only be used by that user.
- All devices supplied must be returned to the University when they are no longer required or prior to the recipient leaving the University, irrespective of how they were purchased (for example, grant funding).

3.3 Third Party Devices

On occasion, staff and postgraduate researchers may be supplied with computing devices by third parties in connection with their research. These devices must be effectively managed, either by the third party, by the University or by the end user. In all cases, the device must meet the minimum security requirements listed above for personally owned devices.

3.4 Remote Working Environment

- When working remotely (either at home or elsewhere), steps must be taken to secure your working environment. Where possible default passwords must be changed for all devices (including personal mobile devices accessing University data and Wi-Fi routers).
- Accessing data classified as Confidential on publicly available devices or networks should be avoided.
- Data classified as Confidential and Sensitive or above must not be accessed on publicly available devices or networks. Publicly available devices and networks include shared computers and wireless networks in public libraries, hotels, cafés or restaurants. When accessing data classified as Confidential or above on public networks, a University VPN connection must be established prior to accessing the data.
- When handling University data classified as Confidential or above, the Information Handling Policy (ISP-07) section 'Information on Desks, Screens and Printers' must be followed.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.

- Do not leave mobile devices unattended in public or unsecured places to minimize the risk of theft.

- Be aware of your surroundings and protect yourself against “shoulder surfing”.

- Reduce the risk of inadvertently breaching UK Data Protection legislation by ensuring that all personal data pertaining to University business, which is subject to the legislation and is stored on the device, is removed before taking the device to a country outside of the European Economic Area that is not deemed to have an adequate data protection regime. See Data and International Travel Guidance for more information on data handling when travelling abroad.

3.5 Reporting the Loss of a Device

The loss or theft of a device that was used to access, process or store University data must be reported to IT Services. This includes all devices whether they are University, personally or third party owned.

For information on loss of University data see Information Handling Policy (ISP-07).

4. Further Guidance

Information Security website:
https://www.bristol.ac.uk/infosec/

Information Handling Policy (ISP-07):
https://www.bristol.ac.uk/infosec/policies/information-handling-policy/

Remote Access Guidance:
https://uob.sharepoint.com/sites/itservices/SitePages/remote-access.aspx

IT Services’ Mobile Devices Support:
https://uob.sharepoint.com/sites/itservices/SitePages/mobile-device-support.aspx

Secretary’s Office’s Guidance on Processing Personal Data Off Campus:
https://www.bristol.ac.uk/secretary/data-protection/guidance/off-campus/#d.en.104703

Password Guidance:
https://uob.sharepoint.com/sites/itservices/SitePages/Passwords.aspx

Data and International Travel Guidance

University’s Information Classification Scheme