University of Bristol
Information Security Policy - Mobile and Remote Working

Title	Mobile and Remote Working
Reference	ISP-14
Status	Approved
Version	1.4
Date created	June 2013
Last reviewed	June 2022
Next review	June 2023
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 and 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 this is often convenient and such use is permitted subject to the following minimum requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access University data and in particular, information classified as confidential or above:

- The device must run a current version of its operating system and must also have a recent security update installed. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- 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 device. The use of biometric authentication methods is also acceptable.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to “autolock” after a period of inactivity (no more than 15 minutes).
- Devices must remain up to date with security patches both for the device’s operating system and its applications.
- Devices that are at risk of malware infection must run anti-virus software.
- Software firewalls must not be disabled or updates postponed. Devices capable of employing a software firewall will typically have this enabled by default and set to automatically update.
- All devices must be disposed of securely, including the removal of University data before disposal, in accordance with the Disposal of Information section of the University's Information Handling Policy.
- The loss or theft of a device must be reported to IT Services.

- Any 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.

In addition to the minimum requirements above, the following recommendations will help further reduce risk:

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

- Consider implementing remote lock/erase/locate features where these facilities are available.

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

- Do not leave mobile devices unattended where there is a significant risk of theft.

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

- Minimise the amount of restricted data stored on the device and do not store any data classified as confidential or above.

- Access restricted information assets via the University’s remote access services (see page http://www.bristol.ac.uk/it-services/advice/homeusers/remote/ for more information) wherever possible rather than transferring the information directly to a device.

- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.

- 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.

- 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.

3.2. University owned devices

The University may at times provide computing devices to some of its members. When it does, it will supply devices that are appropriately configured so as to ensure that they are as effectively managed as devices that remain within the office environment.

Devices supplied by the University must meet the minimum security requirements listed above for personally owned devices.

In addition, 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 research postgraduates 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. In particular, 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, and 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.

3.5. Reporting losses

All members of the University have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any University information asset to the information security incident response team (cert@bristol.ac.uk).

4. Further Guidance References and further guidance University's Information Security website:
http://www.bristol.ac.uk/infosec/

IT Services' Mobile Technology website:
http://www.bristol.ac.uk/it-services/advice/mobile

Secretary's Office's guidance on processing personal data off campus:
http://www.bristol.ac.uk/secretary/data-protection/guidance/off-campus/#d.en.104703

Password guidance:
http://www.bristol.ac.uk/infosec/protectyou/passwords/