University of Bristol
Information Security Policy

Title:	**Mobile and Remote Working**
Reference:	**ISP-14**
Status:	**Approved**
Version:	**1.1**
Date:	**June 2013**
Reviewed:	**November 2014**
Classification:	**Public**

Contents

- Introduction
- Definition
- Scope
- Personally owned devices
- University owned devices
- Third party devices
- Reporting losses
- References and further guidance

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 which are not located on University premises when these devices are used to access University information assets with a classification of confidential or above.

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 which will necessarily result from adopting these permissive approaches. In particular, the University must ensure that any processing of personal data remains compliant with the Data Protection Act.

Definition

A mobile computing device is defined to be a portable computing or telecommunications device which 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 (such as Google Glass).

Scope

This policy applies to all members of the University except for undergraduates and taught postgraduates 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) which are used outside of University premises are also within scope.

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 requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access University information and in particular, information classified as confidential or above:

- The device must run a current version of its operating system. 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. (Some older devices are not capable of encryption and these should be replaced at the earliest opportunity.)

- An appropriate passcode/password must be set for all accounts which give access to the device.

- 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 10 minutes).

- Devices must remain up to date with security patches both for the device’s operating system and its applications.

- Devices which are at risk of malware infection must run anti-virus software.

- All devices must be disposed of securely.

- 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 restricted University information assets.

In addition to the above requirements, 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 (e.g. 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 avoid storing any data classified as strictly confidential.

- Access restricted information assets via the University’s remote access facilities (the “remote staff desktop”) wherever possible rather than directly.

- 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 the Data Protection Act by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).

University owned devices

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

- 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).

Members should also follow the additional recommendations listed above for personally owned devices.

Third party devices

In general, members should not use third party devices to access restricted University information assets. This includes devices in public libraries, hotels and cyber cafes.

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 or 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.

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).

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/dataprotection/depts/dataoffcampus.html