LSHTM Information Management and Security Policy

Supporting policy 6: Mobile and remote working[1]

Approved by Management Board - April 2018

1 Introduction

This Mobile and Remote Working Policy is a sub-policy of the Information Management and Security Policy 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 School premises when these devices are used to access School information assets - in particular those that contain personal or sensitive personal data or LSHTM-confidential data.

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

2 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 and flash/memory cards.

3 Scope

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

4 Personally owned devices

Whilst LSHTM does not require its staff, associates 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 School information and in particular, personal or sensitive personal data or LSHTM confidential information.

4.1 Mandatory requirements

The following are mandatory for all mobile devices:

[1] This document is based closely on a similar at University of Bristol. We are grateful for their permission to make use of the material.

- mobile devices with personal data (as defined in the Data Protection Act 1998/GDPR), including LSHTM emails, must be encrypted - this is likely to be all mobile devices as emails will constitute personal data. 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);

- all devices must be disposed of securely;

- the loss or theft of a device, containing LSHTM data, must be reported to LSHTM information security incident response team (csirt@lshtm.ac.uk);

- 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 LSHTM information assets.

4.2 Recommendations

The following are recommended for all mobile devices:

- the device should 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;

- devices should 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 should run anti-virus software;

4.3 Further considerations

In addition to the above requirements, the following suggestions will help to further reduce risk both to your own information and any LSHTM information on the device:

- 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 - take particular care 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 (see supporting policy 9: LSHTM Data Classification and Handling Policy);

- access restricted information assets via the School’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).

5 School owned devices

The School 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. Unlike personally owned devices which will be managed by their owners, School-owned devices can be managed, to an extent, by LSHTM IT Services.

Devices supplied by the School must meet the minimum security requirements listed above for personally owned devices in sections 4.1 and 4.2.

In addition, the following are required:

- non-LSHTM members (including family and friends) may not make any use of the supplied devices;
- no unauthorised changes may be made to the supplied devices;
- devices must be returned to the School when they are no longer required or prior to the recipient leaving the School.

Members should also follow the additional recommendations listed above for personally owned devices (see section 4.3).

6 Third party devices

In general, members should not use third party devices to access restricted LSHTM 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 School or by the end user. In all cases, the device must meet the minimum security requirements listed above for personally owned devices.

7 Practical help

Advice and guidance is always available from IT Services and guides as to how to carry out the requirements above are available on or from the Information Security website at http://www.lshtm.ac.uk/its/informationsecurity/index.html.

8 Reporting losses

All members of the School have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any School information asset to the information security incident response team (csirt@lshtm.ac.uk). IT Services can then assist in mitigating the data loss - for example, by performing a remote wipe in certain circumstances.

9 Status of this document

This document has been approved by LSHTM's Information Security Working Group and endorsed by Academic Affairs Committee. It is subject to regular review by the LSHTM Information Security Working Group.