London School of Hygiene and Tropical Medicine
Information Security Policy - End User Devices

Document Type	Policy
Document owner	Phil Rogers, Head of Information Security & IT Compliance
Status	Draft
Date Created	August 2023
Approved by	Executive Team
Approval date	
Review date	
Version	1.0
Amendments	
Related Policies & Procedures	https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security

Contents

1. Introduction

This End User Device Policy is a sub-policy of the Information Security Policy and sets out the additional principles, expectations and requirements relating to the use of end user computing devices and other devices not located on University premises when devices are used to access University data.

While recognising the benefits to LSHTM (and its members) of permitting the use of end user 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 end user 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 need 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 LSHTM's Data Classification and Handling Policy which must not be accessed using personally owned devices

The use of personally owned devices is only permitted subject to the adherence to the Bring Your Own Device Policy, and access to LSHTM's systems may be restricted if these are not met.

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 to IT Systems.
- Minimise the amount of University data stored locally on the device and do not access or 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 section 3.2 of LSHTM's Bring Your Own Device Policy for more information: https://www.lshtm.ac.uk/sites/default/files/bring-your-own-device-policy.pdf
- 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 LSHTM's Data Classification and Handling Policy https://www.lshtm.ac.uk/sites/default/files/data-classification-and-handling-policy.pdf

3.2 LSHTM Owned Devices

LSHTM provided computing devices may be used for remote working. These devices are configured to ensure that they are operating effectively and securely at all times via our device management systems over the whole of the devices useable lifecycle.

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, at the end of their useable lifecycle, 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).

- Data classified as Confidential or Highly Confidential 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 handling University data classified as Confidential or Highly Confidential, the Data Classification and Handling Policy 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.

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.

4. Further Guidance

Information Security Guidance:
https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security

Data Classification and Handling Policy:
https://www.lshtm.ac.uk/sites/default/files/data-classification-and-handling-policy.pdf

Hybrid/Remote Working Guidance:
https://lshtm.sharepoint.com/sites/intranet-it-services/SitePages/Hybrid-and-Remote-Working.aspx

Password Guidance:
https://lshtm.topdesk.net/tas/public/ssp/content/detail/knowledgeitem?unid=5516d7ab6d3044a2850c5fdc0e58a1c3

Data and International Travel Guidance