LSHTM Information Management and Security Policy

Supporting policy: Bring Your Own Device Policy

Document Type	Policy
Document owner	Phil Rogers, Head of Information Security & IT Compliance
Approved by	Executive Team
Approval date	23/02/2023
Review date	05/11/2022
Version	2.1
Amendments	05/11/2022 Minor changes and correction.
Related Policies & Procedures	https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security

1. INTRODUCTION

1.1 Personal devices are increasingly used for both work and private functions. They can be a convenient and efficient solution to many work-related tasks. However, without appropriate management there is significant risk for data processed within these systems to be compromised. LSHTM, often processes sensitive data that if compromised could have a severe impact on the organisation, associated organisations and related individuals. Tasking unmanaged, vulnerable personal devices with processing sensitive LSHTM data creates risk that poses a significant threat to the university and its objectives.

1.2 A core responsibility of LSHTM is to ensure processing of sensitive data adheres to legislation, compliance standards, data sharing agreements and organisational requirements. LSHTM is actively engaging with these demands and this policy is a foundational part of this process. This policy provides governance to meet these requirements and is balanced to enable appropriate use of personal devices and the benefits they provide.

1.3 This policy applies to all users that process data directed by LSHTM on all devices not provision, configured and managed by IT Services at LSHTM.

1.4 This policy is issued by Information Governance and Advisory Board.

2. BYOD POLICY – WHO, WHAT, WHY, WHERE AND WHEN?

This policy governs LSHTM data processing on personal devices. Data processing is defined as the collection, recording, organisation, structuring, storage, adaption, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure or destruction of data.

2.1. Who does this policy apply to?

This policy applies to all users that process data for LSHTM on devices not provisioned, configured and managed by IT Services. This includes but is not limited to students, staff and visitors. This policy also applies to those who process data under LSHTM direction, regardless of the user or entity is associated with LSHTM.

2.2. What is BYOD?

Bring Your Own Device (BYOD) is a common term for personal electronic devices used for work functions. These devices include (but are not limited to) smartphones, tablets and laptops. For the purposes of this policy any device that is not provisioned, configured and managed by IT Services is considered BYOD.

2.3. Why is this policy necessary?

This policy is part of the governance that enables LSHTM to pursue its primary organisational objectives. It does this by reducing harmful consequences of poor practice while being flexible by enabling appropriate use of personal devices. It restricts actions that could violate legislation which may generate significant financial penalties and/or reputational damage. It enables the organisation to comply with industry standards which assures external entities considering data sharing agreements or providing funding. This policy addresses any additional requirements directed by LSHTM senior management. It also protects individuals from the negative impact a data breach of their sensitive personal data could inflict. The specific legislation that LSHTM is required to comply with can be found in the Information Management & Security Policy.

2.4. Where does this policy apply?

This policy applies regardless of whether the data is processed in the UK, within Europe or outside. As a data controller based within GDPR jurisdiction, LSHTM is responsible for all data processed under its direction.

2.5. When to use a personal device?

Your options for deciding which device to use and when are defined by the highest classification of the data to be processed. The higher the classification of the data, the greater the restrictions placed upon processing it. Data is classified according to the impact generated if it was compromised. The greater the impact the higher the classification. For further details of LSHTM Data Classification, see the Data Classification Policy. However, the default should always be to use LSHTM managed devices when available.

3. BYOD DATA PROCESSING OPTIONS

3.1. Public and Internal Classified Data

Public and Internal classified data processing can only be conducted on personal devices that comply with the BYOD Configuration Requirements section of this policy. A common example of using Public or Internal classified data on BYOD is the use of personal smartphones to receive LSHTM email. A data breach of this classification should have a low impact on LSHTM. There will be little to no
impact on individuals as there will be no personally identifiable information (PII) compromised.

NOTE: This is only permitted if your email account does not contain data classified as Confidential or Highly Confidential. Email should not be used for sensitive data processing. See the Email Policy for further details.

3.2. Confidential Classified Data

Confidential data must not be processed on devices that cannot be controlled by LSHTM. To access Confidential (but not Highly Confidential) data resources via a personal device there are 2 permitted options:

3.1.1 Virtual Desktop (**Recommended**)
To enable remote working on personal devices (that comply with the BYOD Configuration Requirements in this policy) the virtual desktop service, Horizon is provided. This grants access to LSHTM resources including a suite of applications in a familiar Windows environment. The virtual desktop can be accessed via this link: https://horizon.lshtm.ac.uk This service ensures LSHTM data remains under LSHTM control (and not on personal devices) while increasing the availability of LSHTM resources.

3.2.2 Install LSHTM Security Software (**Avoid if possible**)
To prevent data breaches from the loss of personal devices, organisations commonly implement Mobile Device Management (MDM) services. By installing this software on a personal device LSHTM can be assured that the device adheres to a base level of configuration and can be remotely wiped by the university in the case of theft or loss. Due to the configuration demands on the end user in addition to privacy concerns, this is only recommended if Horizon is not feasible. Note: additional security software may be installed in addition. Contact csirt@lshtm.ac.uk for more information.

If it's not practical to use Horizon due to poor Internet access and installing an MDM client is inappropriate on a personal device, the Service Desk provides a temporary laptop loan service. However, IT requirements must be accurately accounted in funding applications to reduce these complexities.

3.3. Highly Confidential Classified Data

Accessing Highly Confidential data on personal devices is not permitted. Processing this highly sensitive data is rare and designated systems are provided by LSHTM for this purpose.

If you wish to discuss processing this data or there are not approved systems established, contact IT Services.

4. BYOD CONFIGURATION REQUIREMENTS

To process Public or Internal classified LSHTM data, or to securely access Confidential data resources via virtual desktop or on an MDM controlled personal device it must comply with the following:

- All personal devices must be currently supported with security patches and updates.
- Laptops must be protected with a strong password that's not shared or used elsewhere.
- Smartphones and tablets must be protected with an appropriate PIN/biometric/password.
- All personal devices must be fully encrypted.
- Smartphones and tablets must be configured to securely wipe if a PIN/biometric/password is incorrectly entered 10 consecutive times or more.
- A device must never be shared, if it will ever be used to process Confidential or Highly Confidential data.
- Devices must be set to auto-lock within 5 minutes or less of no use.
- Devices must be configured with native remote wipe services if available.
- Smartphones and tablets must only have apps installed from their official stores.
- “Jailbroken” or “rooted” devices must not be used for any LSHTM data access.

- Users must understand what data will be lost in the case of remote wiping.
- Cloud backups (e.g. iCloud on Apple devices) must not include LSHTM data.
- Never stored LSHTM data on personal storage devices (e.g. USB sticks, external drives etc.)
- Never use personal storage device with LSHTM controlled devices.
- All devices must have appropriate anti-virus installed and configured if available.

5. MONITORING

To maintain the confidentiality, integrity and availability of IT services at LSHTM it is necessary to monitor the network and connected systems. When connecting personal devices to the LSHTM network users must be aware and accept there may be logs recorded of that connection. Only necessary and proportionate monitoring is conducted for the maintenance and security of LSHTM assets.

If a personal device is configured with LSHTM security software (e.g. an MDM client) users must be aware and accept additional device activity may be logged. It is recommended for usability and security reasons to choose the remote desktop Horizon if practicable rather than the MDM option. This is additionally recommended if users have privacy concerns.

6. FURTHER INFORMATION & ASSISTANCE

For IT advice and help contact the Service Desk.

For general information security requests and notifications contact csirt@lshtm.ac.uk

To report a potential data breach contact dpo@lshtm.ac.uk

7. VERSION CONTROL

Version Number	**Author/Reviewed by**	**Approved by**	**Purpose/Change**	**Date**
1.0	Jim Nicholas	Management Board	Initial policy	04/03/2020
1.1	Abu Hossain (Information Security Manager)		Policy review	24/06/2021
2.0		Management Board		30/06/2021
2.1	Abu Hossain – Information Security Consultant	Executive Team	Policy Review	23/02/2023