End User Device Policy

Document Type	End User Device Policy
Document owner	Azim Khan, Head of Operations and Support
Approved by	Executive Team
Approval date	13/03/2025
Review date	March 2026 (annual review) March 2028 (triennial review)
Version	2.0
Amendments	Full rewriting of policy from 2023 – main amendments: Removal of Personally Owned devices sections Added section on User Responsibilities More detailed section on Device Management Full detail on expected Device Lifecycle
Related Policies & Procedures	Information Security Policy Acceptable Use Policy

1. SUMMARY

Device Provision: Staff and RD's are typically issued a single laptop. Taught course students must provide their own. Staff and students must only use their LSHTM device where provided, and not a personal one.

Shared Desktop Computing Facilities: Shared desktop PCs are provided in specific environments like lecture theatres, labs, and flexible working spaces for doctoral students.

Mobile Devices: Mobile devices, including phones and tablets, are provided to support research and administrative functions based on role requirements.

User Responsibilities: Users must adhere to LSHTM's Information Security and Acceptable Use Policies, ensure device security, report loss or theft, and return devices upon leaving LSHTM.

Device Lifecycle: The lifecycle includes specification, procurement, onboarding, visibility and updating, maintenance, and support, with a focus on security and compliance.

Device Management: to ensure compliance with data security, standardize configurations, and facilitate software distribution and support.

2. SCOPE

This document relates to all user computing devices (laptops, desktop PCs, tablets and smartphones) that are provided by IT Services to London-based LSHTM staff and doctoral students. For other types of LSHTM staff such as visitors or honorary where a LSHTM device is not provided, or for students such as MSc or Short course students, these are otherwise referred to LSHTM's Bring Your Own Device (BYOD) policy.

3. PURPOSE AND OVERVIEW

The purpose of this document is to establish standards and provide a framework for the provision, lifecycle and management of end user computing devices. The document provides an overview and does not aim to go into specific technical details. The text should be read in conjunction with other LSHTM policies, such as those dealing with procurement and data security.

4. POLICY

4.1. Device Provision

4.1.1. Overview

LSHTM staff are typically issued with a single laptop computer, for their exclusive use. These can be used together with a monitor and dock that are available in designated work areas or where staff have requested these for home working. Staff and students must **only** use their LSHTM device, and not personal one, where provided.

- The single laptop is provided for working both on and off site, offering the most flexible solution for hybrid working and efficient platform for communication.
- Some roles may require an additional device such as a mobile phone, tablet, access to a shared desktop resource or a higher specification device.
- New doctoral students as of January 2024 are provided with similar equipment, however taught course students will be required to provide their own hardware.
- Devices are funded by faculty or central services budgets, or through a specific project or research grant where eligible. The device is considered as belonging to LSHTM where it has been purchased using any of the above LSHTM-related funds.
- Eligibility for an LSHTM-provided device (such as a laptop or mobile phone) should be discussed with the member of staff's line manager and budget holder within their department or faculty.
- Devices much be purchased via IT Services, who will advise on the specification and assist with procurement as required.

4.1.2. Shared desktop computing facilities

Shared desktop PCs may be provided for a number of specific computing environments to augment individual laptop use. Examples include:

- **Lecture theatres and teaching rooms** are equipped with a desktop computer to facilitate presentations by staff and visiting lecturers.
- **Laboratory environments** which often have specific and unique requirements for dedicated workstations and configurations, such as for use with microscopes and other lab equipment. Some devices are owned and managed by LSHTM; others are provided and maintained by third party companies.
- **Flexible working spaces** for doctoral students, which might otherwise only offer a docking station and monitor, may additionally provide a number of shared desktop computers for students who have not previously been issued with an institutional laptop. The library also oversees the current eLibrary space in Keppel Street which has a small number of fixed desktop computers which are provisioned and supported by IT Services.
- **Estate management and specialist use cases**. Some environments may require fixed workstations, such as for building security systems, reception, catering, and in cases where a dedicated PC might be required to run software to connect to a particular hardware device such a scanner or specialist printer.

4.1.3. Mobile devices

Android or Apple mobile devices are provided to support research and administrative functions. These include:

- **Mobile phones -** these are provisioned to LSHTM staff based on the requirements of their role;
- **Data collection devices -** typically, Android tablets for use in field projects;
- **Handheld devices** - for dedicated functional use. For example, Android phones for building security staff.
- **Miscellaneous tablets -** supported devices purchased for auxiliary business use.

4.1.4. Virtual computing

- LSHTM also provides access to virtual desktops through Horizon and the High Performance Computing (HPC) service. These are hosted in LSHTM's data centre and provide solutions for hybrid working, remote access, data processing and specialist computing requirements for research and group teaching.

4.2. User Responsibilities

- Users must adhere to LSHTM's Information Security and Acceptable Use Policies.
- Users must comply with all software licensing agreements.
- Users must not allow their device to be used by anyone other than themselves.
- All devices must be secured by PIN, password or other means when not in use or away from desk.
- If any device is lost or stolen, or is believed to show signs of compromise, it must be reported immediately to csirt@lshtm.ac.uk or the IT Services Helpdesk.
- All reasonable measures must be taken to minimise the risk of loss, theft, damage or avoidable physical wear to any device.

- Users must not tamper with or attempt to defeat any security measures that have been put in place to secure their device.
- Staff must run updates in a timely way when prompted by their operating system to ensure the on-going security of their device. IT Services may additionally request that devices be made available to them for essential updates, software refreshes, or replacement.
- Staff and students must return all devices to LSHTM when they cease to be a member of LSHTM and in accordance with LSHTM's leaver procedure and fixed asset policies

4.3. Device Lifecycle

4.3.1. Specification

- **Hardware choice**. New devices are typically chosen from a predefined list, however some flexibility is offered where needed for someone to perform their role effectively. Specification for any new equipment will take account of use case requirements such as workload, software prerequisites, anticipated lifetime, accessibility and occupational health requirements, portability, durability, environmental footprint and budget. Staff or students approaching IT Services with requirements for high spec devices will be advised of virtual computing options available where appropriate.
- **Peripherals**. Monitors, docking stations, keyboards, mice and headsets for both onsite or working for home, are purchased from a standard list, with similar consideration being given where variation is required and requests can be raised with IT Services where a particular requirement is identified. Webcams, external microphones and speakers are not typically required for laptops. Portable storage devices such as USB sticks and external hard drives are not offered as their use would typically be in breach of the LSHTM's Information Security policy.
- **Operating system**. Windows based laptops are provided by default, offering the greatest compatibility with LSHTM systems and best value for money. Apple Mac computers can be selected as an alternative where appropriate for the role and use case. Support is also extended to Linux. For mobile phones and tablets, Android is considered by default, although iPad and iPhone options can also be provided.

4.3.2. Procurement

- All hardware, software and peripheral devices must be purchased through LSHTM's Procurement system. Purchases made personally will not be reimbursed via expenses and should not be purchased using an LSHTM credit card. Such devices will not be set up or supported by IT Services. Exceptional cases where standard procurement routes are not feasible (e.g. some fieldwork overseas) should be discussed with IT Services and the Procurement Team in advance of purchase to agree an acceptable approach.
- All devices must be sourced exclusively from the LSHTM's incumbent manufacturer or supplier. This enables LSHTM to benefit from
    - Cost savings through volume purchasing discounts.
    - Streamlining of support and warranty arrangements.

    - Supplier's ability to pre-enrol devices into the LSHTM's IT management systems using Autopilot (Windows) or ADE (Apple).
- In exceptional circumstances devices from other institutions may be considered for onboarding, such as when an external research group joins LSHTM.

4.3.3. Onboarding

- All computers, smartphones and tablets will be enrolled in their respective IT management system.
- All IT purchases will be recorded centrally in IT Service's asset database.
- Every asset will be given an identity and database record that is unique, exclusive and immutable.
- A designated primary user will be recorded as the keeper of every single-user device (typically laptops and mobile phones). Shared devices may be assigned to specific projects, research groups, departments, or physical locations where appropriate. Associated assets such as monitors and docking stations for off-site use will also be assigned to individual users.
- A physical label will normally be applied to every LSHTM asset to aid identification and to denote ownership by LSHTM.

4.3.4. Visibility and updating

- IT Services will maintain the ability to individually query warranty and purchase records, and locate assets by device name, serial number, assigned user or location.
- A device management system will provide detailed device properties such as make, model, hardware specification, MAC address, OS version, current user, encryption status, etc.
- Asset records for all devices will be updated by IT Services when changes occur in assigned user, location, lifecycle state (in use, spare, disposed, lost, etc).

4.3.5. Maintenance and support

- IT Services provides full support for all devices belonging to LSHTM. No liability is accepted for personally owned computers and only basic advice and guidance can be given. Staff must use an LSHTM device where provided and are otherwise referred to LSHTM's Bring Your Own Device (BYOD) policy
- IT Services provides a walk-up, online and phone helpdesk service for device-related queries, troubleshooting, and support.
- All new devices are covered by manufacturer warranties. Repairs are coordinated through IT Services. Non-warranty repairs will be undertaken on a best endeavours basis and may be chargeable to the end user's department or grant in circumstances such as physical damage or expired warranty.

4.3.6. Refresh and replacement

- There is typically no fixed age at which a device is routinely replaced. It will depend on the specification, circumstances, reliability, environmental impact, funding available, or when the device can no longer be supported. Devices are usually expected to last at least five years.

- Devices withdrawn on specified regular refresh cycles will be considered for redeployment to replace older units within the organisation that do not have a clearly defined refresh schedule.
- Ageing hardware cannot be supported indefinitely. LSHTM users are encouraged to seek a replacement for their hardware before it becomes obsolete, inefficient or can no longer reasonably be supported. Users should speak to their line manager/supervisor or Department manager in the first instance.

4.3.7. Redeployment

- When a member of staff or Research Degree student leaves the organisation, any devices, including laptops, mobile phones and other hardware they were using must be surrendered back to their parent project or department and then returned to IT Services for the device to be assessed for either retirement or redeployment. It is the responsibility of the staff member or Research Degree student to return the device(s) and for the respective line manager to ensure this happens.

- To adhere to security requirements, any computer being transferred to another user will have its OS reset or re-imaged so that the device is effectively redeployed as a new machine.

4.3.8. Decommissioning

- All end user computing devices must be returned to IT Services for disposal when a device reaches the end of its functional life.
- Any licensed software that has required activation will be de-activated before the device is retired.
- Asset records will be updated to record all devices being retired from use.

4.3.9. Disposal

- All devices will be securely wiped of all data before disposal. This may be done either in house, although is more typically achieved through an accredited third-party supplier.
- All equipment will be disposed responsibly in accordance with WEEE regulations.
- Devices must not be retired for home use at the end of their life. This practice is at odds with data security policies, software licensing terms, WEEE regulations, electrical safety liability and can generate unrealistic support expectations.
- In exceptional circumstances where ownership is transferred to another organisation, the device will either be reset to factory specification, or otherwise securely wiped of all data and not hold any LSHTM licensed software.

4.4. Device Management

IT management systems exist to ensure that all devices comply with LSHTM's data security and authentication policies, adhere to audit and licensing obligations, standardise configuration across the estate, provide a flexible and secure solution for distribution of software, and facilitate support and troubleshooting by IT staff.

4.4.1. Enrolment

- All new and existing devices will be enrolled into one of the LSHTM's IT management systems.
- Windows devices are automatically pre-enrolled for Autopilot by the supplier in the LSHTM's Microsoft Entra ID tenant. Existing devices may also be enrolled retrospectively.
- MacOS and iOS devices are automatically enrolled by the supplier into Apple's Automated Device Enrolment programme.
- Samsung Android devices are pre-enrolled by the supplier into Samsung's Knox platform.

4.4.2. Software and system deployment

- All new end user computing devices will be deployed with the operating system pre-installed by the manufacturer.
- The pre-installed operating system, together with the manufacturer's device drivers and other system utilities will typically form the basis of a Standard Operating Environment (SOE).
- The SOE will include a device management agent, a portal for software installation and any additional security utilities required. Essential productivity tools (such as Microsoft Office 365 and a standard PDF file reader) will be preinstalled or made available through the designated software portal.
- Additional LSHTM-licensed and commonly used software will also be provided through the designated portal and should not typically require any privilege elevation to install.
- Legacy devices or equipment required for special use cases may be deployed with an alternative predefined operating system and software configuration.

4.4.3. Login and authentication

- All standard end user computing devices must be configured to require some form of authentication for access. This might take the form of traditional username and password, PIN, swipe pattern or biometric/smart card authentication.
- All new Windows devices will routinely be joined to the LSHTM's Microsoft Entra ID tenant, requiring modern multi-factor user authentication such as Windows Hello for Business. Legacy Windows endpoint might alternatively be joined to the LSHTM's internal Active Directory infrastructure and therefore require online or offline AD credentials for access.
- Use of local login accounts are only to be considered in circumstances where more secure authentication methods are impractical or unavailable. Local user accounts may exist on legacy configurations to enable IT staff to assist with troubleshooting and support.

4.4.4. Device and data security

- Enforcement of device configuration required for LSHTM security policies (drive encryption, system update schedule, device lock, etc) will be implemented through respective IT management systems. Additional measures, such as restrictions to limit boot options and guard against unauthorised repurposing may also be adopted.

- Additional software to provide security measures such as enhanced threat protection, auditing and compliance remediation may routinely be deployed over time.