UNIVERSITY OF GLOUCESTERSHIRE

University of Gloucestershire
Library, Technology & Information Service

Mobile and Laptop Device Policy

LTIU-POL-14

Document Control

Issue/Amendment Record

Issue	Date of Issue	Reason for Issue
1	August 2018	Major Revision
2	02/01/20	Review

Document Ownership

	Name and Title	Signature	Date
Author	**Dan Smale** Head of Technical Delivery		02/01/20
LTI Approval	**Rob Blagden** Director LTI Service		02/01/20
Release Authority	**Robin Livesey** Content Support & Information Manager		02/01/20

Introduction

The University of Gloucestershire (the "**University**") is committed to providing a safe and secure environment, where students, staff, visitors and contractors can use technology to support their study/work and development.

This policy lays out the purchasing, acceptable use and responsibilities applicable to mobile devices to ensure safe and appropriate use of University of Gloucestershire mobile assets. In addition it outlines the authority for IT staff to conduct audits on mobile devices to investigate or ensure compliance with University policies, or other legal or contractual requirements.

Members of staff who manage computer systems on behalf of the University must familiarise themselves with this policy.

This policy may be amended from time to time as deemed appropriate. Please check back frequently to see any updates or changes to this policy.

Type of Policy

Administrative Policy

Purpose

The University has an obligation to ensure that its assets are protected and being operated in line with policies.

Mobile computing devices (laptops, tablets, phones, etc) are inherently at greater risk of loss, or infection from malware, due to their nomadic nature, and may be exposed to multiple IT infrastructures beyond the University's control (i.e. home, public WiFi, hotels / conferences, etc).

In addition, mobile devices are valuable assets, which are the target of thieves or those looking to acquire information.

To mitigate these risks, mobile endpoint devices are required to be audited regularly. These audits will be conducted to:

- Investigate known or suspected security breaches.
- Monitor conformance with the Information Security Policy and other legal or contractual requirements.
- Ensure possession of assets
- Provide updates to bring the asset inline with current working practices, technical controls, or policies

Scope

This policy applies to:

- Any mobile phone, smart phone, laptop, tablet, or other portable IT equipment that is University owned or operated – herein referred to as a "device", unless explicitly stated otherwise.

- All users (students, staff or contractors) or administrators of the above IT equipment.

Accountable Owner

- All devices shall be registered to an accountable owner, who has responsibility for the device.

- The LTI Service shall maintain the register of device owners.

- Accountable ownership also applies to devices available for loan or shared as part of a pool.

- Where ownership changes, the LTI Service IT and Library HelpDesk must be notified, as any unusual or suspicious use of a mobile device will be referred to the accountable owner.

Purchasing

- All devices must be procured through the LTI Service

- Requests for new equipment must be directed through the LTI Service IT and Library HelpDesk, along with budget holder approval

- Purchasing must be from the list of preferred devices (latest list available from the LTI Service IT and Library HelpDesk or your campus LTI Senior Technician).

- If a user has a need for a specific make or model that is not on the preferred list they should contact the LTI Service IT and Library HelpDesk for guidance.

Audit

- Device owners will periodically be contacted by a member of the LTI Service, and shall agree and date, time and location at which they will present their device for audit.

- Device owners must present their device as agreed – failure to present the device will constitute a breach of this policy

- The LTI Service shall:

- Maintain the details of the device, associated owner, and when the device was last seen
- Progress any device maintenance. This may include:
  - Updates, or patches
  - Install of any required software (i.e. anti-malware)

Special Situations

- Where an audit uncovers a potential criminal matter, the audit must be stopped immediately, and the device will be quarantined. The Chief Information Officer or a designated representative will be informed, and the Police notified.

Downloading of Free Applications

- By default, smart phones devices will be configured to enable a user to download and install applications. For other devices the installation of software will need to be done through an LTI Service Technician.
- Some free applications enable storage of University data in third-party party systems, e.g. Dropbox, or present significant security risks. Before installing a new application the user should check the latest guidance from their campus LTI Senior Technician. At all times it is the user's responsibility to be aware of the risks of any installed applications and to seek advice if in doubt.
- As a general guide, users should avoid the use of third-party applications that enable connectivity to University systems (e.g. use of non-standard email clients) due to the information security threats posed. Please read the guidance for help as above or contact the LTI Service IT and Library HelpDesk.

Purchasing Paid-For Applications

- The default route for purchasing applications should be through the LTI Service purchase route. The user should raise a request with the LTI Service IT and Library HelpDesk identifying the application, the number of copies required, the devices to be installed on and the budget information
- Where appropriate, the LTI Service may facilitate accounts for Schools/Departments that will enable local purchase and management of applications and mobile devices
- In all cases, users should take care to note the terms and conditions that apply to applications

Protections

- Security policies are applied to devices to provide protection against unauthorised use and the potential of the device being misplaced, lost or stolen.

- For smartphone devices this includes:
  - Device PIN of at least four digits (changeable by the user)
  - Automatic password lock at a maximum of five minutes
  - Wipe of the phone's memory after ten failed password attempts
  - Encrypted as standard

- Where possible encryption will be applied to a device to protect data contained on the device from accidental loss, theft, etc.

Updates

- Users shall not prevent centrally-provisioned updates from being installed and shall accept any prompts for installation.

- Users shall reboot their devices when necessary to do so to fully install patches or updates.

Support

- The LTI Service is available to help with setup, use and problems associated with devices.

- The replacement or repair costs are the responsibility of the original budget holder unless the device ownership has transferred or otherwise agreed with the LTI Service.

Device Loss

- A user must contact the LTI Service Library and IT HelpDesk immediately if they are aware of the loss of a mobile device. In this event, the LTI Service will take appropriate action, up to and including wiping the mobile device and advise the user of other actions that should be undertaken (e.g. University password change).

- Where a user has used their personal device to access University systems and has University accounts or protected information stored on the device, then in the event of loss the LTI Service Library and IT HelpDesk must be contacted as soon as possible for guidance.

Insignificant Personal Use

- Devices are supplied to users for primarily business use

- It will be assumed that no personal taxable benefit is derived where the personal use of the item is deemed to be insignificant. This is in line

with the requirements of The Income Tax (Earnings & Pensions) Act 2003,section 316, which covers the business and personal usage of items made available to employees

- Where is it deemed that the personal use is significant, then a taxable benefit will arise and the employee will be subject to a tax charge

- Significant Personal Use would be considered as any of the following:
    - Downloading personal software onto a device
    - Using GPS navigation systems for a significant number of private journeys
    - Holding personal photos and other personal files on the device
    - Using the device to store/play personal music files
    - Frequent personal internet access
    - Holding personal e mail accounts on a device

- To verify that staff are meeting the requirements of this guidance, and therefore are not subject to a taxable benefit, users sign and agree that they understand and agree to abide by the University's insignificant use guidelines for the device with which they have been issued.

Sanctions

- Contravention of this policy may lead to action according to the relevant conduct and discipline procedures through HR or a user's line manager, including deactivation or withdrawal of the device.

Exceptions

- Any exceptions to this policy shall be discussed and agreed in writing with the LTI Service.