Bring Your Own Device Policy (BYOD)

Version 1.0

Effective from 04/04/2025

Contents

1 Purpose

The purpose of this policy is to define the requirements that personally owned devices (devices that are not owned by the university) must meet if they are used to access university IT resources including:

- Data
- Applications and services
- Computer systems

In accordance with the Information Security Policy, some of the university IT facilities and services are sensitive (Confidential) and should only be available when logged into using an IT Services centrally managed and supported device e.g. Managed Windows Service. IT Services applies carefully maintained policies and security controls to these devices to safeguard the resources they can connect to.

Accessing University IT resources from a personally owned device is referred to as 'Bring Your Own Device' (BYOD). IT Services has no control over the configuration of BYOD. It is therefore the responsibility of the device owner to apply relevant security controls to their device to minimise the risk to university data and systems.

This policy is subsidiary to the IT Acceptable Use Policy which outlines acceptable and prohibited use of University of Liverpool IT facilities and services, regardless of whether the device is University or personally owned. This policy also supports and enforces the requirements of the Information Security Policy and the Data Protection Policy.

2 Scope

This policy applies to all users of university IT facilities and services with an MWS account accessing University IT resources from a personally owned device (BYOD). This includes:

- Laptops and workstations
- Mobile phones
- Tablets.

3 Policy Statements

3.1 BYOD required controls

a. **Device PIN / Password:** Access to the device must be controlled with a 6 character PIN or password. It should not be possible to unlock the device without authentication. Biometric authentication may also be used.
b. **Anti-malware protection:** Antimalware protection must be active and up to date on all Windows or MacOS desktop or laptop computers.
c. **Encryption**: Device encryption protects data in case the device gets stolen. It must be enabled within the device system preferences or settings.
d. **Supported hardware and software:** The device, its operating system and all applications must be supported and appropriately licensed.

e. **App Stores:** Only install software from reputable sources. Android and Apple devices can only install apps from the official app stores by default. Do not bypass this control in order to install apps from untrusted sources.

f. **Software / application updates:** Your device must be kept up to date. Operating system and application updates should be installed promptly.

g. **Rooting / jailbreaking:** Mobile device operating systems are locked down so that users can only make certain configuration changes. Circumventing these restrictions is called "rooting" (on an Android device) or "jailbreaking" (on an Apple device). Rooted or jailbroken devices must not be used to access University resources.

h. **Device firewall:** Enable the host firewall on desktop and laptop computers.

3.2 BYOD User Responsibilities

a. Take practical measures to protect your BYOD from loss or theft.

b. If your BYOD is lost or stolen and it may access University data or systems, report it via the IT Services self-service portal: https://servicedesk.liverpool.ac.uk. Incidents relating to university personal data should be reported immediately via your line manager and Data Protection Officer.

c. Before leaving the University, or selling their device, BYOD users must ensure no University data remains on the device.

d. Public wi-fi networks and hotspots may not be adequately protected, meaning that traffic from your device may be visible to other users of the network. Do not access University IT resources or carry out activities such as online banking or shopping while connected to public wi-fi.

3.3 BYOD limitations/prohibited access

The University of Liverpool require that a university owned, centrally managed and supported device e.g. MWS, (which meets security requirements) must be used when accessing highly sensitive information, back-office system access or completing an infrastructure systems admin role (i.e. with elevated and privileged rights).

BYOD must not be used for the following purposes:

- **Privileged Access**. It is not permitted to use any account with elevated administrative privileges from a BYOD. Privileged access must be from a managed, university-owned device.
- **Administrative access to business systems**. BYOD must not be used to access administrative functions of university business systems. This includes:
  - Personnel / HR systems
  - Finance systems
- **Storage of highly sensitive data**. Any data classified as Confidential (in accordance with the Information Security Policy) must not be stored on BYOD.

4 Policy Compliance

All use of and access to University IT facilities and services (including access from BYOD) is logged and subject to monitoring, investigation and breach as defined in Section 3.0 of the IT Acceptable Use Policy (see Section 6 Related Documentation).

5 Exception Process

Any exceptions to this policy will be subject to a request, review and approval process by IT Services. The exception process will be handled on a case-by-case basis.

6 Related Documentation

This section lists policies that are relevant when accessing University IT facilities.

Public Policies

- JANET (UK) Connection, Security & Acceptable Use Policies
- IT Acceptable Use Policy (AUP) - Acceptable and prohibited use of university IT facilities & services
- Information Security Policy – Framework for security of university information
- Data Protection Policy – Data Protection controls
  - Staff-related Policies including Staff Disciplinary
  - Research-related Policies including Research Misconduct
  - Student-related Policies including Student Conduct & Discipline and Academic Integrity

Internal University policies and procedures

- Network Access Policy - Rules for connecting a device to the university network (wired or wireless)
- VPN Policy – Rules for connecting a device to the university Virtual Private Network (VPN)
- Infrastructure Management Code of Practice - Rules for using a University owned device (that is not centrally managed by IT Services)

Guidance and Forms

- IT Services webpages: https://www.liverpool.ac.uk/it/
- IT Services self-service portal: https://servicedesk.liverpool.ac.uk

7 Policy Document Control

Policy Version Control *(most recent version first)*			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Senior Cyber Security Analyst R. Humby	New document outlining rules for use of BYOD	1.0	Information Governance Committee: 12/03/2025 IT Services SMT: March 2025
Policy Management & Responsibilities			
Owner	This policy is owned by the Director of IT Services. The Director has the authority to issue and communicate policy on IT facilities and services including information security priorities and has delegated responsibility for the day-to-day implementation and communication of the policy to Head of IT Security team and will be supported by IT Services teams.		
Policy Enquiries	Please direct any queries about this Policy to the IT Services self-service portal: https://servicedesk.liverpool.ac.uk		
Policy Review Due: 6 months by Sep 2025.			
Document Location:	IT Services webpages https://www.liverpool.ac.uk/it/regulations/ University Policy Centre https://www.liverpool.ac.uk/policy-centre/		
** The Owner & Author are responsible for publicising this policy document. **			