Digital Services

Students & Alumni: Bring Your Own Device (BYOD) Policy

Contents

1. Document Control

Title	Student: Bring Your Own Device (BYOD) Policy
Version	1.1
Review date	October 2026
Summary of changes	Responsibility change from 1) Chief Digital Information Officer to Deputy COO and Director of Business Operations 2) Head of Cyber Resilience to Head of Cyber & Information Security 3) Information Services to Digital Services
Policy live date	November 2025
Policy owner	Deputy Chief Operating Officer (DCOO) & Director of Business Operations
Stakeholders consulted in development	IS SLT & Managers College IT (CDEPS, CBASS, CHMLS) Data Privacy Information Assurance Committee
For information & action	All students & alumni
Supersedes	N/A
Supporting policies	• IT Acceptable Usage Policy • Data Protection and Information Access Policy • Information Classification Policy • Password Policy

2.   Purpose and Background

2.1   The purpose of this policy is to outline the University's requirements for students and alumni with regards to the use of personally owned devices, also known as Bring Your Own Device (BYOD), to access information and services provided by the University, for the proper stewardship of the use of these assets and for the security of information accessed while using such devices.

2.2   The use of BYOD poses a security risk as they are not managed by the University, may not be patched, or running adequate anti-virus software, and are likely to be more vulnerable to unauthorised access. Individuals are also more likely to have admin rights on their personally owned computer which increases the risks from malware.

2.3   The following BUoL policies should be referenced in conjunction with this Policy:
   - IT Acceptable Usage Policy
   - Password Policy
   - Data Protection and Information Access Policy
   - Information Classification Policy

3.   Scope

3.1   The definition of BYOD covers user endpoint devices that are not owned by the University.

3.2   This Policy applies to all students and alumni using their own device to connect to the BUoL network and/or information systems, either on-site or remotely.

4.   Definitions

Authorised Device	A user endpoint device that has been registered and approved to access the University's network and/or systems.
Alumni	Former students of BUoL.
Availability	Information and systems available when needed.
BYOD	'Bring Your Own Device' use of a device that is not owned by BUoL to access BUoL information systems and data. E.g. personally owned devices, third party owned devices.
BUL Network Account	Main account used to access BUL email, network services and cloud applications.
Confidentiality	Only permitting authorised access to information, while protecting from improper disclosure.
Cloud Applications	Software delivered to users over the Internet.
Business Service Owner	A senior-level individual or the designated department within BUoL that holds ultimate accountability for a specific dataset or data domain.
Information	All information and data held on BUoL's applications and systems.
Information Security Management System (ISMS)	A framework of policies and controls that manage security and risks systematically across the entire organisation. Typically aligning with a common security standard e.g. ISO 27001
Information Services Team	The Information Services Team at Brunel encompassing the Information Services Directorate and College IT Teams.
Information Systems	BUoL's systems, devices, services (e.g. Internet, email, "bring your own device" (when connected to the University systems) and telephony, applications, and information in logical and physical form as well as any other University equipment. This also includes service providers' systems/equipment when provided to BUoL.
Integrity	Information is recorded, used, and maintained in a way that ensures its completeness, accuracy, consistency, and usefulness for the stated activity.
May/Should	Refers to items regarded by BUoL as minimum good practice, but for which there is no specific legal requirement.
Personal Data	Information relating to a Data Subject, who can be identified directly or indirectly from that information. Personal Data can be factual (such as name, email address) machine data (such as IP Address, device information), or an opinion about that person's actions or behaviour. It does not include anonymised data.
Personally Owned Device	Includes - but is not limited to – laptops, personal computers, netbooks, tablets, and smartphones that are used to collect, store, access, transmit, carry, use, or hold any University data. It applies to the use of the Personally Owned Device both during and outside of normal working

	hours and whether or not it is used at your normal place of work.
Students	All individuals enrolled on a course of study at BUoL (undergraduates, postgraduate research, executive students)
University Confidential	Information only available to a limited number of individuals and requiring a stringent level of security protection.
User Account	An account assigned to an individual to access a system.
User Endpoint Device	Laptops, notebook computer, desktop, tablet, mobile phone
We	Brunel University of London (BUoL)
Will/Shall/Must	Equals 'is required to'. It is used to indicate mandatory requirements to be strictly followed to conform to the standard and from which no deviation is permitted.
Zero Trust	A security model requiring every access request to be fully authenticated and authorised before granting access.

5.   Policy Statement

5.1   Key Principles

The University permits the use of student and alumni BYOD for access to and processing of BUoL information, but this must be in accordance with the BUoL IT Acceptable Usage Policy.

The contents of BUoL systems and information accessed from BYOD remains BUoL property. This covers all materials, data, communications and information transmitted to, received or printed from, or stored or recorded on BYOD during the course of your studies at BUoL, regardless of who owns the device.

BUoL will not have access to personal data on BYOD, such as private messages, photos, or personal apps. BUoL will only manage and secure work-related applications, data, and settings to ensure compliance with security policies, while personal information held on the device remains private and unaffected.

All University information accessed via BYOD must be handled in line with the BUL Information Classification Policy.

In accordance with the BUoL IT Acceptable Usage Policy, University protected/confidential or personally identifiable information must not be downloaded from University applications or systems to BYOD/personal cloud storage.

BUoL information held on BYOD is subject to the Freedom of Information Act 2000 and Data Subject Access rights under the UK GDPR and the DPA 2018 and must be provided to BUL Information Services Team on request.

BYOD accessing BUoL network and information systems must be registered and approved before access is granted. Once registered BYOD that has not accessed the network and information systems for over 90 days will be required to re-register to gain access. On transfer to Alumni status, BYOD will be automatically de-registered from University systems.

BUL reserves the right to carry out audit activities at any time on device connections and to prevent access to the University network or services from any device that is considered a risk.

BUL Information Services Team will never remotely access a BYOD. This is to safeguard both the user device and the University.

BYOD costs are the responsibility of the user, including but not limited to voice and data usage charges and any purchase, updating and repair costs.

5.2   Policy Framework

This Policy is part of BUoL's Information Security Management System and should be read in conjunction with the BUoL IT Acceptable Usage Policy, BUoL Data Protection & Information Access Policy and any other relevant policy as mentioned in this document.

5.3 Accountability

Brunel's Deputy Chief Operating Officer (DCOO) & Director of Business Operations has overall accountability for this policy.

The DCOO will be accountable for implementing and enforcing this Policy, ensuring that access controls are in place and aligned with this Policy.

5.4 Key roles & responsibilities

Head of Information Security

The Head of Information Security is responsible for the production, maintenance and communication of this Policy and has overall responsibility for maintaining and ensuring compliance against this Policy.

BUL Digital Services Team

BUoL Digital Services Team will implement technical controls and procedures to enforce this Policy.

It is the Information Services Team's responsibility to ensure that the infrastructure is secure and compliant to all relevant Acts and laws.

Note: *BUoL Digital Services Team will provide guidance and advice on how to connect personal devices to University services; however, we do not offer technical support or troubleshooting for personally owned equipment.*

Students and Alumni

All BUoL students and alumni are expected to always comply with the controls defined within this Policy in accordance with BUoL's IT Acceptable Usage Policy.

5.5 Exemptions

Where it is not possible to apply or enforce any part of this policy, then a request detailing the reason(s) why it is not possible must be raised with the IT Service Desk in the first instance. BUoL's Head of Information Security will review the business justification and advise on the associated risks. Policy exceptions will only be issued when the relevant Business Service Owner has signed off on the identified risks.

5.6 Policy Review and Maintenance

This Policy and all supporting policies and procedures that form BUoL's Information Security Management System (ISMS) will be reviewed and updated on an annual basis to ensure that they:

- Remain operationally fit for purpose;
- Reflect current technologies;
- Are aligned to industry best practice; and
- Support continued regulatory, contractual, and legal compliance.

6.   Device Protocols

Student and alumni BYOD must meet the following requirements to access BUoL systems and information:

- **Password Protection:** to prevent unauthorised access, the device must at minimum have either password, pin or pattern protection enabled, with fingerprint or face ID enabled if available. **Device passwords and pins must be a least six characters in length.**

- **Auto lock-out:** the device must have automatic lock features enabled. Ensuring if left unattended the device will automatically place itself into a lock state, requiring the password to be entered to unlock. **The time out must be set to a maximum of fifteen minute.**

- **Operating systems and applications:** only standard operating systems may be used, any altered version such as 'rooted', 'jailbroken', or equivalent are strictly forbidden from accessing the BUL network and information systems.

  Device operating systems and applications running on the device must be fully supported by the manufacturer and on the latest version where possible. Devices running end of life/unsupported operating systems and applications will not be permitted access to the BUL network and information systems.

- **Protection:** where available the device must have modern security protections in place, such as local firewall enabled, anti-virus software installed and up to date, it is also recommended that file sharing is turned off. In addition, users are responsible for maintaining their device by ensuring it is regularly patched and upgraded using updates provided by vendors.

- **Network Protection:** the device must not be used to access University confidential information over unsecured networks, including public WiFi networks.

  The below conditions must always be met to ensure compliance with the BYOD policy:

- **Network Access:** only registered BYOD devices are authorised to connect to the BUoL wireless network. Wired access to the BUoL network is only permitted on the University Residential Network.

- **Software:** BUoL licenced software is only allowed to be installed onto BYOD if permitted within the licencing terms.

  BYOD must only use licensed software and applications, obtained from legitimate sources, to minimise the likelihood of interception and compromise of University information systems, and malware infection.

  All BUoL licenced software must be removed from BYOD on completion of studies.

- **Loss or theft:** loss or theft of BYOD, or where University confidential information may have been accessed by an unauthorised person or otherwise compromised, must be reported to the IT

Service Desk within 24hrs, in accordance with the BUoL IT Acceptable Usage Policy. **University data held on BYOD will be remote wiped should the device be lost or stolen.**

- **Completion of Studies:** on leaving BUoL or when disposing of or selling BYOD, all University confidential data (incl. email, apps, and files) must be deleted securely from the device. Students must follow the University's Research Ethics Process, with regards to data that must be removed from their device on completion of their studies with the University.