BISHOP GROSSETESTE UNIVERSITY

Document Title:	**IT Services**: Bring Your Own Device (BYOD)	
Document Category:	Policy	
Version Number:	1.0	
Status:	Approved	
Reason for development:	Remote Working, Mobile working, Visiting Tutors, Hourly Paid Lecturers, End Point assessment, staff and students using their own device(s).	
Scope:	This policy applies to University staff, students, partners, and authorised consultants	
Author / developer:	Head of IT	
Owner	Chief Operating Officer	
Assessment: (where relevant)	☒Equality Assessment ☐Legal	☒Information Governance ☐Academic Governance
Consultation: (where relevant)	☒Staff Trade Unions via HR ☒Bishop Grosseteste University Students' Union ☐Any relevant external statutory bodies	
Authorised by (Board):	Finance, Employment & General Purposes Committee	
Date first authorised:	24 February 2021	
Date current version authorised:	24 February 2021	
Date current version effective from:	1 April 2021	
Date next review due to commence:	1 April 2022	
Document location:	University website	
Document dissemination / communications plan	This document will be disseminated to all staff and students within the University via the website	
Document control:	All printed versions of the document should be classified as uncontrolled. The controlled version will be available on the University website / SharePoint	
Alternative format:	If you require this document in an alternative format, please contact governance@bishopg.ac.uk	

***Please note, this document remains valid until formally revoked or replaced by the University.**

IT Services: Bring Your Own Device (BYOD) Policy

1. Introduction

1.1. This policy covers the use of non-University owned digital devices which are used to access University services, systems, products, data, and information. Devices include, but are not limited to personal smartphones, tablets, laptops, PCs, Macs, portable media devices and similar technologies.

1.2. If you use your own device to access University services, systems, and information you may do so, provided you follow the provisions of this policy and the advice and guidance provided through the IT Services Helpdesk.

1.3. The University intends to put in place as few technical and policy restrictions as possible for a BYOD subject, enabling the University to meet its legal and duty of care obligations.

1.4. The University, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a user, you are required to keep the University's information and data secure. This applies to information held on your own device, as well as University devices. You are required to assist and support the University in carrying out its legal and operational obligations, including co-operating with IT Services should it be necessary to access or inspect University information stored on your device.

1.5. The University reserves the right to refuse, prevent or withdraw access to users, devices, services, or products where it considers that there are unacceptable IT security risks related to University business, its staff, students, reputation, services, or infrastructure.

1.6 This policy should be read in conjunction with the University's IT *Services Acceptable Use Policy* and *IT Security Policy* available at https://www.bishopg.ac.uk/wp-content/uploads/2018/05/IT-Systems-Acceptable-Use-Policy.pdf

The policy will be subject to review, in line with University guidelines.

2. Definitions

2.1 **BYOD** - Bring Your Own Device refers to users using devices or services which are not owned or provided by the University, to access and store University information, whether at the place of work or remotely, typically connecting to the University's wireless network, Virtual Private Network (VPN), or virtual desktop.

2.2 **Portable Device** - Hand-held and mobile IT equipment which is used for accessing, storing, or processing University information, including laptops, PCs, Macs, tablets, and smartphones.

2.3 **Portable Media** - Readily-transportable items used to store information in digital form (whether temporarily or long-term), including USB memory sticks ("flash drives"), memory cards, smartphones, compact discs (CDs and DVDs), plug-in external drives, and media players (mp3 players).

2.4 **Data Controller** - The University, as data controller, determines the purpose for processing any personal data, in the context of this policy.

2.5 **User** – A member of staff, enrolled student, partner, contractor, visitor, or another person authorised to access and use the University's services.

3. Service, Device, Portable Media, and Information Security

3.1. The use of your own device must adhere to the University's *IT Services Acceptable Use Policy* and *IT Security Policy*.

3.2. When you use your own device as a work resource, you must maintain the security of the University's information you handle (which includes but is not limited to viewing, accessing, storing, or otherwise processing).

3.3. From time to time, the University may require that you install or update University-approved device management software on your own device.

3.4. It is your responsibility to familiarise yourself with your device sufficiently to keep data secure.

In practice this means:

- Preventing theft and loss of data (using Biometric/PIN/Password/Passphrase lock).
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

3.5. You must **not** retain personal data and confidential information from University services on your own device or media. If you are in any doubt as to whether data can be stored on your device you are required to err on the side of caution and consult with your line manager, information governance, or seek advice from the IT Services Helpdesk.

3.6. You must:

- Use the device's security features, such as a Biometric, PIN, Password/Passphrase, and automatic lock to help protect the device when not in use.
- Keep the device software up to date, for example using Windows Update, Software Update Services, and App updates.
- Activate and use encryption services, anti-virus protection, and anti-malware on your device.
- Activate hardware-based encryption on portable media devices (USB memory sticks etc) with software to set up and manage the passphrase. If it cannot be encrypted, it must not be used.
- Install and configure tracking and/or remote wiping services, such as Apple's 'Find My iPhone', Google's 'Find My Device' or Microsoft's 'Find My Device', where the device has this feature.
- Remove any University information downloaded and stored on your device immediately after you have finished accessing and using it including any copies of e-mail attachments, documents, spreadsheets, presentations, reports, and data sets, etc.
- Limit the number of emails and other information that you are syncing to your device to the minimum required, for example only keep the past 24 hours of email in sync.
- Remove all University information from your device and return it to the manufacturer's settings before you sell, exchange, or dispose of your device.

3.7. If your device is lost, stolen or its security is compromised, you must promptly report this to the IT Services Helpdesk, so they can assist you to change the password to all University services (it is also recommended that you reset passwords for any personal services that have accessed via that device, e.g., social networks, online banking, online shopping, etc). You must cooperate with University IT staff in wiping the device remotely, even if such a wipe results in the loss of your own information and data, such as photos, contacts, and music.

3.8. You must not attempt to circumvent the device manufacturer's security mechanisms in any way, for example, to 'jailbreak'[1] an Apple device or 'root'[2] an Android device.

3.9. Further advice and guidance on securing personal devices is available from the IT Services Helpdesk.

[1] See http://en.wikipedia.org/wiki/IOS_jailbreaking
[2] See http://en.wikipedia.org/wiki/Android_rooting

4. Monitoring of User Owned Devices

4.1. The University will not monitor the content of your devices; however, the University reserves the right to monitor and log data traffic transferred between your device and University services, both over internal networks, VPN, and accessing University services via the Internet.

4.2. In exceptional circumstances, for instance where the only copy of a University document resides on a personal device, or where the University requires access to comply with its legal obligations (e.g., under the Data Protection Act 2018, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) the University will require access to University data and information stored on your device. Under these circumstances, all reasonable efforts will be made to ensure that the University does not access your private information.

4.3. Under some circumstances, for example, where you legitimately need to access or store certain types of information, such as student or financial records on your device, you must seek authorisation from your line manager. The University may then need to monitor the device at a level which may impact your privacy by logging all activity on the device. This is to ensure the privacy, integrity, and confidentiality of that data.

4.4. You are required to conduct work-related, online activities in line with the University's *IT Services Acceptable Use Policy*.

5. Use of personal cloud storage services

5.1 Personal data, as defined by the Data Protection Act (2018) and University confidential information may not be stored on personal cloud services[3] and you should only use the University provided Microsoft OneDrive for business as part of Microsoft 365 which you access using your University IT account logon.

6. Compliance sanctions and disciplinary matters

6.1 Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the University's disciplinary policy.

7. Help, advice, and support

7.1. Where possible the University supports all devices, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy.

7.2. Support for your own device is offered on a reasonable endeavour's basis, with advice and guidance on all aspects of this Policy available via the IT Services helpdesk:

Web: https://helpdesk.bishopg.ac.uk
Email: helpdesk@bishopg.ac.uk
Phone: 01522 583666

7.3. The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

7.4. Additional advice and guidance on Data Protection legislation is available from the University's Information Governance team or online via the UK government website.

[3] I.E. Apple iCloud, Dropbox, Google Drive, Microsoft Personal OneDrive, Box, etc.

BISHOP GROSSETESTE UNIVERSITY

8. Other supporting documents

IT Acceptable Use Policy
IT Security Policy
JANET Acceptable Use Policy