Bishop Challoner
Sixth Form College

BYOD

BRING YOUR OWN DEVICE

STUDENT POLICY

CONTENTS

1. INTRODUCTION

This Bring Your Own Device (BYOD) policy outlines the guidelines and expectations for the use of personal devices by students at Bishop Challoner Catholic College. BYOD refers to the practice of allowing individuals to bring their own laptops onto the school premises for educational purposes. This policy aims to ensure the safe and responsible use of personal devices while maintaining a secure and productive learning environment. This policy aligns with the Department for Education (DfE) Digital Standards and relevant legislation, including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

2. POLICY OBJECTIVES

a) Encourage the use of personal devices to enhance learning, collaboration, and communication.
b) Promote equality and inclusion, enabling all students to benefit from BYOD.
c) Promote digital literacy, responsible digital citizenship, and effective digital skills among students.
d) Ensure the promotion of e-safety and digital well-being, aligning with DfE's emphasis on safeguarding.
e) Safeguard sensitive information and protect the school's network infrastructure from security threats.
f) Establish clear guidelines to ensure fair and equitable access to resources and minimize distractions during instructional time.

3. SCOPE AND APPLICABILITY

a) This policy applies to all students who bring their personal devices onto the school premises.
b) All students must adhere to this policy when connecting their devices to the school network or accessing school resources on the Internet.
c) All students should understand that the Acceptable Use Policy guidelines are also applicable to the use of personal devices on the school premises and must adhere to that policy.
d) Parental consent is required for students to participate in BYOD.

4. DEVICE REQUIREMENTS

a) Students must ensure their devices meet minimum security standards, including up-to-date antivirus software and security patches.
b) Devices must be registered with the school's IT department to gain network access.
c) Students are responsible for maintaining the integrity and functionality of their devices.
d) Specific technical requirements or preferred devices will be defined to ensure compatibility and security.
e) It is recommended to have insurance for personal devices. The school's insurance policies will not cover personal devices against loss or damage.

5. NETWORK AND INTERNET ACCESS

a) Students must only connect to the school's network through the designated wireless network provided.
b) Students must only use their own username and password to connect to the designated wireless network. The ICT Support Team should be informed if usernames and passwords are unknown.
c) Network security measures will be implemented to protect the school's IT infrastructure. Students should understand that their devices will only be able to access the Internet through the designated wireless network. No access to internal file server storage or printers will be permitted. Students must refrain from attempting to gain access to any of these resources.
d) Internet access through the school network will be filtered to protect students from harmful content, in line with DfE guidelines. Students must refrain from accessing, or trying to gain access to inappropriate or illegal content.
e) The school reserves the right to monitor network traffic and block access to specific websites or services where deemed necessary.
f) Bandwidth-intensive activities such as streaming videos or downloading large files should be limited to non-instructional hours.
g) The use of personal mobile data networks should be minimized to prevent unnecessary charges. The school is not liable for any charges for data use.

6. DATA AND PRIVACY

a) Students are responsible for ensuring the security and privacy of their personal data stored on their devices.
b) Students should exercise caution when sharing sensitive information and follow the school's data protection guidelines.
c) Unauthorized access, sharing, or distribution of personal or confidential information is strictly prohibited.
d) The school is not liable for any loss, damage, or unauthorized access to personal data stored on personal devices.
e) Compliance with the Data Protection Act 2018 and UK GDPR is required.

7. RESPONSIBLE USE AND DIGITAL CITIZENSHIP

a) Inappropriate or disrespectful use of personal devices is strictly prohibited, including cyberbullying, harassment, or accessing and sharing inappropriate content.
b) Students should not use their devices to record audio or take photographs or videos of other students or members of staff without their permission.
c) Students should report any incidents of misuse or breaches of this policy to the appropriate authorities.
d) Ongoing digital literacy education will be provided, covering topics like cyberbullying, online safety, and responsible use.

8. CLASSROOM USE AND DISTRACTIONS

a) Devices should be used in a manner that supports educational activities and does not disrupt the learning environment and should support the curriculum.
b) Teachers may establish specific rules regarding device usage during instructional time.
c) Students must respect the instructions provided by teachers and staff regarding device usage in the classroom.

9. DEVICE SUPPORT AND MANAGEMENT

a) Students are responsible for the setup, maintenance, and troubleshooting of their own devices.
b) The school's IT department may provide limited technical support for connecting to the school network or accessing school resources on the Internet.
c) The school is not responsible for any physical damages or loss of data resulting from device support or maintenance.

10. NON-COMPLIANCE AND SANCTIONS

a) Failure to comply with this policy may result in disciplinary action, including but not limited to the revocation of network access privileges or other appropriate measures.
b) Serious breaches of this policy may be reported to the appropriate authorities if necessary.
c) Disciplinary actions for non-compliance will be consistently enforced and clearly communicated to students and parents.

11. POLICY REVIEW

a) This BYOD policy will be reviewed periodically to ensure its effectiveness and alignment with evolving technologies, best practices and DfE Digital Standards frameworks.

BYOD Specification Guide

RECOMMENDED MINIMUM HARDWARE (FOR WORD PROCESSING AND INTERNET BROWSING)

Screen Size	This is a personal preference, but it is recommended the minimum screen size is 10" so that students can make effective use of the tools available on a suitably sized screen.
Processor (CPU)	Minimum 2 Cores, Recommended 4-6 Cores
RAM	Minimum 4GB, Recommended 8-16GB
Local Storage	Minimum 128GB (1TB of cloud storage is provided via the school Microsoft accounts).
Battery Life	Battery life should last the school day having charged overnight. The school cannot offer chargers.
Wireless	Dual Band 802.11a/b/g/n/ac – ax 5GHz
Antivirus	The device MUST be maintained with up-to-date antivirus software

HIGH END RECOMMENDED HARDWARE (FOR MEDIA/GRAPHICS)

Screen Size	This is a personal preference, but it is recommended the minimum screen size is 14" for media/graphics processing.
Processor (CPU)	Recommended 4-6 Cores minimum
RAM	Minimum 8GB, Recommended 16GB+
Local Storage	Minimum 500GB (1TB of cloud storage is provided via the school Microsoft accounts).
Battery Life	Battery life should last the school day having charged overnight. The school cannot offer chargers.
Wireless	Dual Band 802.11a/b/g/n/ac – ax 5GHz
Antivirus	The device MUST be maintained with up-to-date antivirus software

OPERATING SYSTEM

The following Operating Systems (OS) will work with the BYOD scheme, however it is highly recommended that students are working on a Windows OS since the school systems use Microsoft software and services.

- Windows 10 or 11 with most recent releases and updates (Home, Pro, Education and Enterprise versions). The school cannot license users for Windows OS, so users must ensure that their devices have the appropriate license.
- Apple OSX (MacBook OS) with most recent releases and updates. This will include MacBook Air's from 2020 and MacBook Pro's from 2018 onwards.

SOFTWARE

The school's email system is Microsoft 365 and as such, users have license to insall Microsoft 365 Apps for Business on up to 5 devices for free through their school email account.

Any software that students use on their devices should be paid for and licensed where required. The school does not recommend software piracy. Students at the school are allowed to use Canva and Adobe Express online for free with their school email accounts. However, students are responsible for licensing any other software that is downloaded and installed on their personal devices.

SUGGESTED ACCESSORIES

- Headphones, to minimise disruption to others during lessons and in shared study spaces.
- It is strongly recommended that a sturdy protective case or sleeve is used to transport personal devices.
- The school is not responsible for any damages to personal devices, so some form of insurance cover would also be recommended.

ANTIVIRUS SOFTWARE

Windows devices that use Windows 10 or 11 Operating Systems arrive with Microsoft Defender Antivirus. At a minimum, this should be used as antivirus software and kept up-to-date.

Recommended Antivirus Software: Avast, Panda, Microsoft Defender

Unrecommended Antivirus Software: Any software that is shipped with a device, as these are usually just free trials. These include Kaspersky, Norton, McAfee. It is recommended to uninstall these!

Apple devices are generally considered secure due to the way the Operating System is written and how devices operate. However, antivirus software is still available for added protection. Avast or Bitdefender for Mac would be recommended.

SMART PHONES AND OTHER UNSUPPORTED DEVICES

Apple iOS, Android and Windows phone devices are not supported by the BYOD scheme and should not be connected to the wireless networks provided at the school. Please refer to the school's phone policy for the use of smart phones and mobile phones.

Acceptance of BYOD Policy for Students

Student Agreement

As a prospective participant of the school's BYOD scheme, I have read and understand the BYOD Policy for Students. If I do not follow the guidelines and expectations, I understand that this may result in loss of access to the BYOD network provided by the school, as well as other disciplinary action.

Student Name:	
Form Group:	
Signature:	
Date:	

Parental Agreement

As the Parent/Carer of the student named above, I have read and understand the BYOD Policy for Students and agree to the guidelines and expectations under which my CHILD will be permitted to use their personal device on the school premises.

Parent/Carer Name:	
Parent/Carer Signature:	
Date:	

Bishop Challoner
Sixth Form College