BRING YOUR OWN DEVICE POLICY

NAMED PERSON:	Mr Richard Peel Deputy Headteacher

Last Review Date:	September 2026
Review Cycle:	2 Years
Next Review Date:	September 2028

Mr Andy Crossey **Chairman of Governing Body**
Signed: A.D. Crossey
Date: September 2026

RELATED POLICIES:

- Online Safety Policy, (incorporating Acceptable Use Agreements)

CONTENTS

1. Personnel responsible for this policy
2. Connecting devices to School systems
3. Monitoring and filtering
4. Lost or stolen devices

APPENDICES:

- Appendix 1 – Declaration & Agreement

1 OVERVIEW AND SCOPE

We recognise that many of our students have personal mobile devices which they could use for learning purposes. This policy applies to all students on roll at The Buckingham School and visiting Sixth Form students. It covers the use of devices to access our IT resources and communications systems both during and outside School hours whilst on the School site. All students must agree to the contents of this BYOD policy via signature before they are permitted to use their own device.

2 PERSONNEL RESPONSIBLE FOR THIS POLICY

The Senior Leadership Team has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the IT Services provider. IT Services provider and the School Governors shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

IT Services provider has responsibility for ensuring that any person who may be involved with administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

All staff and students at The Buckingham School are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the IT Services provider. If you have any questions regarding this policy or have questions about using your device for learning purposes which are not addressed in this policy, please contact the IT Services provider.

This policy applies to students who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for learning purposes. It applies to the use of the device both during and outside School hours whilst on the School site. This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, PDAs, tablets and laptop or notebook computers, including Chromebooks.

When you access School systems using a device, the School is exposed to a number of risks, including the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device). This could result in damage to School systems. The purpose of this policy is to protect School systems while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of School systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

Breach of this policy may lead to the School revoking your access to School systems, whether through a device or otherwise. It may also result in sanctions up to and including exclusion. You are required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

Some devices may not have the capability to connect to School systems. The School is not under any obligation to modify its systems or otherwise assist students in connecting to those systems.

3 CONNECTING DEVICES TO SCHOOL SYSTEMS

The school operates distinct device requirements and technical setups depending on the student's year group to ensure network security and appropriate access.

Years 7–11:

- Device Requirement: Students in Years 7–11 are encouraged to bring Chromebooks, which are considered an important tool for lessons and tutor group time.
- Management and Setup: These students must purchase a Chromebook and pay for a license which adds them to the school's Google Workspace environment. The school fully controls these devices; they are locked down, and this is the only way they are permitted to operate on the school network.
- Registration: For Years 7–11, the serial number of the device will be recorded along with owner details and stored securely on the school's internal system.
- Software: In order to access school systems securely, it may be necessary for IT Support to install software applications on devices belonging to Year 7–11 students. If a student removes any such software, their access to the systems will be disabled.

Years 12–13 (Sixth Form):

- Device Requirement: Sixth Form students are permitted to use a wider variety of devices, including laptops, netbooks, tablets, and smartphones.
- Connection: Students using Android and Windows devices will join the Wi-Fi using their Active Directory (AD) credentials.
- Chrome Devices: Because Chrome devices do not authenticate in the same way, Years 12 and 13 students using Chrome devices will join on a segregated network.
- Exemptions: We do not record device details for Years 12 and 13, and the school will not install any software on these personal devices.

4 MONITORING AND FILTERING

To protect school systems and ensure compliance with KCSIE and the School's Safeguarding Policy, the school strictly manages internet traffic. Devices will only access the internet through The Buckingham School network.

- Filtering (All Students): The school maintains appropriate filtering systems to block harmful and inappropriate content—such as illegal materials, extremism, and pornography—without unreasonably impacting teaching and learning. All devices across all year groups go through the school's filtering systems.

Monitoring (Differentiated):

- Years 7–11 are fully integrated into the school's active monitoring platform to prevent misuse and ensure compliance with our standards of conduct.
- Years 12–13 do not have the active monitoring platform, though they remain subject to the overarching filtering systems.

By signing this policy, students confirm their agreement to the school inspecting devices, and remotely reviewing, copying, disclosing, or wiping data if there is a suspected breach of security.

5 APPROPRIATE USE AND SECURITY

- Educational Use: Devices will only be used for educational purposes to support learning whilst in School, and it is at the teacher's discretion as to when they may be used.
- Media and Privacy: Students will not use their device to record audio or take photographs or video of other students or members of staff without their permission.
- Online Safety: Students must adhere to the school's Online Safety Policy. They must not access inappropriate material, engage in cyber-bullying, or share indecent/explicit images.
- Responsibility: Students are responsible for the adequate security of their own device whilst in School, keeping it with them at all times. Devices should be fully charged at home; charging in school is only permitted with a PAT tested charger.

6 LOST OR STOLEN DEVICES

Lost, Stolen, or Damaged Devices Students bring devices into School entirely at their own risk. The Buckingham School will not accept any responsibility for devices that are misplaced, lost, stolen, or damaged. In the event of a lost or stolen device, students should report the incident to their Head of Year and the Student Office. It is highly recommended that devices are fully insured and have location finder apps enabled.

7 TECHNICAL SUPPORT AND COSTS

- No Technical Support: Consistent across all age groups, we do not provide technical support for personal devices.
- Costs: Students and parents are responsible for all repairs, maintenance, replacement costs, and device services. For usage of a Chromebook in Years 7-11, the cost of the license for adding to the system must be paid through the school before the IT team enroll. Usage of the device in school may increase personal data usage charges, which the student alone is responsible for.

8 DEPROVISIONING DEVICES

When a student leaves the school, the Chromebook is able to be deprovisioned from the school system to be used without the restrictions on:

- An email needs to be sent by the parent or guardian to chromebooks@buckinghamschool.org including the student's name and Chromebook Serial number
- The IT Support team will then check with the Data office to ensure the student is officially off-role
- The IT Support team can then remotely deprovision the device and trigger a factory reset, returning it to a clean device without the school restrictions on.

9 BREACHES OF THE POLICY

If a student breaches this BYOD Policy, the Online Safety Policy, or the ICT Acceptable Use Policy, they may be subject to sanctions up to and including exclusion.

- Members of staff have the right to access, search, and confiscate a student's device if there is reasonable grounds to suspect it poses a risk, is evidence of an offence, or violates policy.
- In exceptional circumstances, authorised staff members may examine and erase data or files if there is a 'good reason' to do so to prevent harm or disruption.
- Subsequent breaches will result in the temporary or permanent removal of network access and the revocation of BYOD privileges.

APPENDIX 1

DECLARATION & AGREEMENT (TO BE SIGNED BY ALL STUDENTS)

I wish to use my personal mobile device for learning purposes at The Buckingham School

- I have read, understood and agree to all of the terms contained in the Bring Your Own Device to School Policy.
- I acknowledge and agree that authorised personnel of The Buckingham School shall have the rights access, monitor, review, record and data contained on my personal device if a breach is suspected.
- I understand that if I breach this policy, my device may be removed and investigations carried out.

_____

SIGNED (STUDENT)

_____ _____

PRINTED NAME and TUTOR GROUP **DATE**