



ROBERT CLACK SCHOOL

BRING YOUR OWN DEVICE POLICY

If printed, copied, or otherwise transferred from this website this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time. Please consult the Policies page on the website for the latest update

Controlled Document

Title	Bring Your Own Device Policy
Author	Data Protection Officer
Owner	Headteacher
Document Version	Version 4
Created	August 2026
Approved by	Approved in accordance with the School's governance arrangements
Review Date	August 2029 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control:

Version	Date	Author	Description of Change
1	12/01/2021	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	New Policy
2	20/01/2022	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	GDPR 2016/679 to UK GDPR
3	01/08/2023	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Policy review
4	August 2026	Data Protection Enterprise Ltd www.dpenterprise.co.uk	Policy Review. Amendments to: S1,2,3,5,6,7,8 and 10

Contents:

1. Introduction
2. Policy statement
3. Roles and responsibilities
4. Access to the school's internet system
5. Access to the school systems
6. Monitoring the use of personal devices
7. Security of staff personal devices
8. Compliance with data protection policy
9. Support
10. Safeguarding considerations
11. Compliance, sanctions and disciplinary matters for staff
12. Incidents and reporting
13. Policy review
14. Links with other policies

1. INTRODUCTION

This policy applies to staff and visitors. Arrangements relating to pupil use of personal devices, including mobile phones and other connected technology, are addressed separately within the School's Behaviour Policy, Online Safety Policy and Acceptable Use Policy.

The School recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. Our School embraces this technology but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by staff and visitors to the School of non-school owned electronic devices to access the internet via the School's internet connection or to access or store school information. This practice is commonly known as 'bring your own device' or BYOD. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy, please check with the school's network or business manager. These devices are referred to as 'personal devices' in this policy.

This policy is supported by the school's Acceptable Use Policy.

2. POLICY STATEMENT

Staff should keep personal use of personal devices to a minimum during working hours and should only use such devices where this does not interfere with their duties or create safeguarding, confidentiality or professional conduct concerns.

Visitors to the School may use their own personal devices in the following locations:

- In designated areas with staff supervision
- In the classroom with explicit permission of the teacher
- In designated common areas such as reception, corridors or meeting rooms.

Staff and visitors to the School are responsible for their personal devices at all times. The School is not responsible for the loss or theft of, or damage to the personal devices or storage media on the device (e.g. removable memory card) howsoever caused. The School reception must be notified immediately of any damage, loss, or theft of a personal device, and these incidents will be logged.

Personal devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

Personal devices must not be used to take photographs, video or audio recordings of pupils, staff, visitors or school activities unless expressly authorised by the Headteacher or another senior leader and in accordance with the School's safeguarding, acceptable use and data protection policies.

The School reserves the right to refuse staff and visitors permission to use their own personal devices on school premises.

3. ROLES AND RESPONSIBILITIES

Staff members will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of school information
- Install relevant security features and maintain the device appropriately
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used
- Set up remote wipe facilities if available, and implement a remote wipe if the device is lost/stolen
- Encrypt documents or devices as necessary.
- Report the loss of any device containing school information, or any security breach immediately to the School Data Protection Officer
- Ensure that no school information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party.

Visitors will:

- Familiarise themselves with the use of personal devices at school
- Only use personal devices for agreed purposes at the School and with the relevant permission
- Not share information from personal devices via social media and will not keep school information indefinitely.
- Not use the record facility unless permission is sought and provided.
- Cease using a personal device or leave the premises if required, where its use give rise to safeguarding, security or confidentiality concerns.
- Comply with safeguarding requirements, including restrictions near children

4. ACCESS TO THE SCHOOL'S INTERNET CONNECTION

The School provides a wireless network that staff and visitors to the School may use to connect their personal devices to the internet. Access to the wireless network is at the discretion of the School, and the School may withdraw access from anyone it considers is using the network inappropriately.

The School cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The School is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the School's wireless network. This activity is taken at the owner's own risk and is discouraged by the School. The School will have no liability whatsoever for any loss of data or damage to the owner's device resulting from the use of the School's wireless network.

All internet access through school networks is subject to filtering appropriate to the school's safeguarding requirements. Staff and visitors acknowledge that browsing activity may be logged and reviewed.

5. ACCESS TO THE SCHOOL'S SYSTEMS

School staff are permitted to connect to or access the following school services from their personal devices:

- The School email system (where appropriate encryption technologies have been deployed);
- The School virtual learning environment (Google Classroom, Office 365 and 'School Drives');
- Official school applications

Staff may use the systems listed above to view school information via their personal devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their personal devices. In some cases, it may be necessary for staff to download school information to their personal devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it. Where personal or sensitive data is used in this way devices or files **MUST** be encrypted.

Staff must only use the IT services listed above (and any information accessed through them) for work purposes. School information accessed through these services is confidential, in particular information about pupils. Where personal data is transmitted by email, staff must ensure that only the minimum necessary information is shared and that appropriate security measures, including encryption where appropriate, are used. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the School Business Manager (or equivalent) and the School Data Protection Officer as soon as possible in line with the School's Data Protection Policies.

Staff must not send school information to their personal email accounts.

If in any doubt the user should seek clarification and permission from the School Network Manager (or equivalent) before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the School systems.

6. MONITORING THE USE OF PERSONAL DEVICES

The School uses technology that detects and monitors the use of personal and other electronic or communication devices, which are connected to or logged on to the School wireless network or IT systems. By using a personal device on the School's IT network, staff and visitors to the school understand that monitoring is carried out for security, safeguarding and network management purposes. The School's use of such technology is for the purpose of ensuring the security of its IT systems and for tracking school information.

The information that the School may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms. Information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the School internet connection should report this to the School's Network Manager (or equivalent) as soon as possible.

7. SECURITY OF STAFF PERSONAL DEVICES

Staff must take all sensible measures to prevent unauthorised access to their personal devices, including but not limited to the use of a PIN pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time. Staff that wish to use their own device must be aware that they have a direct personal responsibility to ensure that the device they choose to use has the benefit of encryption.

Personal devices may only be used to access approved school systems, applications and services. Staff must not use personal devices to access or store school information through unauthorised applications, cloud storage services or personal accounts.

Staff must never attempt to bypass any security controls in school systems or on own devices. Staff must ensure that appropriate security software is installed on their personal devices and must keep the software and security settings up to date.

Staff must ensure:

- passwords are kept securely and are not accessible to third parties. Automated log on processes to store passwords must not be used
- Devices have remote wipe capability activated
- No photographic capability may be used on school premises without explicit headteacher permission
- Device screens must not be visible to pupils during lessons unless part of planned teaching activity
- Camera and recording functions must be disabled in changing areas and private spaces

Staff are reminded to familiarise themselves with the School's e-safety and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

8. COMPLIANCE WITH DATA PROTECTION POLICY

Staff compliance with this BYOD policy ensures the School meets its obligations under:

- UK GDPR and Data Protection Act 2018
- Education legislation regarding pupil data protection
- Data Use and Access Act 2025 (DUAA) where relevant and where applicable provisions have been brought into force.

All personal data must be processed in accordance with the school's privacy notices and pupil data may only be accessed for legitimate educational purposes. Any data breach must be reported to the School Data Protection Officer immediately.

Where such devices are used to process data of a personal or sensitive nature appropriate encryption of files or devices must be used. All such data should be backed up to the School's network or school's Google or Office 365 accounts and deleted from personal devices as soon as work has been completed.

9. SUPPORT

The School cannot support users' own devices but will offer advice to users in their use where practically possible.

The School takes no responsibility for supporting staff's own devices or has the responsibility for conducting annual Portable Appliance Testing (PAT) of personally owned devices.

10. SAFEGUARDING CONSIDERATIONS

This policy operates within the School's safeguarding framework:

- All device use must comply with Keeping Children Safe in Education guidance
- Staff must report any inappropriate content involving minors immediately
- Visitor device use near children is restricted and monitored
- Any concerns about inappropriate device use should be reported through safeguarding channels.
- All use of personal devices must support and comply with the School's filtering and monitoring arrangements and online safety requirements.

11. COMPLIANCE, SANCTIONS AND DISCIPLINARY MATTERS FOR STAFF

Non-compliance of this policy exposes both staff and the School to risks. If a breach of this policy occurs the School may discipline staff in line with the School's Disciplinary Procedure. Guidance will also be offered to staff to support them in complying with this policy. If steps are not taken by the individual to rectify the situation and adhere to the policy, then School may require the member of staff to cease using the device on school premises and may temporarily secure the device where necessary as part of a safeguarding, security or disciplinary investigation. For persistent breach of this policy, the School will permanently withdraw permission to use user-owned devices in school.

Examples of serious breaches include:

- Unauthorised sharing of pupil data via personal devices
- Use of unsecured cloud storage for school information
- Failure to encrypt sensitive data as required
- Breach of security protocols
- Use of devices for inappropriate content in school environment

12. INCIDENTS AND REPORTING

The School takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of a personal device should be reported to the School office in the first instance. Data protection incidents should be reported immediately to the School's Data Protection Officer.

13. POLICY REVIEW

The DPO is responsible for monitoring and reviewing this policy. Although this policy is reviewed every three years, changes to legislation, national guidance, codes of practice or advice from the Information Commissioner advice may trigger interim reviews. The DPO will highlight any significant legislative developments that may require earlier action or updates to this Policy.

The School is aware of the upcoming Data Use and Access Act 2025, and this policy will be reviewed should any changes be brought into force affecting this policy.

14. LINKS WITH OTHER POLICIES

This Bring Your Own Device Policy is linked to the School:

- Data Protection Policy
- Freedom of Information Policy
- Security Incident and Data Breach Policy
- Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Staff Code of Conduct

The Information Commissioner provides a free helpline and a wide range of guidance and resources relating to information rights and data protection. Further information is available from: [Information Commissioner Office \(ICO\)](#)