John Perry Primary 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.

Approved by: School Governing Body **Date:**

Last reviewed on: August 2024

Next review date: August 2027

Controlled Document

Title	Bring Your Own Device Policy
Document Type	Approved
Author	Data Protection Officer
Owner	Headteacher
Subject	Bring Your Own Device (BYOD)
Document Version	Version 3
Created	01/08/2023
Approved by	Governing Board
Review Date	August 2027 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. Amendments to: S1 – Added reference to AUP S1 – Headteacher amended to read SBM/IT Manager S2 – Office amended to Reception S2 – Added recording meetings S3 – Bullet point 4 added S6 – Headteacher amended S7 – Sentence added S9 – Sentence deleted

Contents:

1. Introduction
2. Policy Statement
3. Roles and Responsibilities
4. Access to the School's Internet Connection
5. Access to the School's Systems
6. Monitoring the use of Personal Devices
7. Security of Staff and Personal Devices
8. Compliance with Data Protection Policy
9. Support
10. Compliance, Sanctions and Disciplinary Matters for Staff
11. Incidents and Reporting
12. Policy Review
13. Links with other Policies

1. INTRODUCTION

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 must only use personal devices in the staff room, or in an office, during free time, unless as part of a planned lesson.

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

- In the classroom with the permission of the teacher
- In the School environs

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.

Recording of any conversation/meeting on a personal device is not permitted by staff or visitors unless prior notice is given in advance and consent is given.

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.

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.

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. Emails should not name individual pupils and any attached documents containing personal details of pupils, should be encrypted. 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 agree to such detection and monitoring. 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 (including passwords). 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.

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 that passwords are kept securely and are not accessible to third parties. Automated log on processes to store passwords must not be used.

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 is an important part of the School's compliance with the Data Protection laws. Staff must apply this BYOD policy consistently with the School's Data Protection guidelines.

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. 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 the personal device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the School will permanently withdraw permission to use user-owned devices in school.

11. 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.

12. POLICY REVIEW

The Data Protection Officer is responsible for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

13. 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

The Information Commissioner also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk