PENK VALLEY ACADEMY TRUST

BYOD (bring your own device) Statement of Policy

Adopted by Trustees:	
Signed:	
Date:	**Spring 2026**
This policy is reviewed annually by the Audit and Risk Committee.	
Next Review date:	**Spring 2027**

COLLABORATION CHALLENGE CURIOSITY CARE

POLICY INFORMATION

Date of last review:	Spring 2026	**Review period:**	Annually
Date ratified by Trustees:	Spring 2026	**Trustee committee responsible:**	Audit Finance and Risk
Policy owner:	Chief Operations Officer	**Executive team member responsible:**	Chief Operations Officer

Reviews/revisions

Review date	Changes made	By whom
Spring 2025 Spring 2026	Policy created. No changes	LMC LMC

Equality and GDPR

All Penk Valley Academy Trust policies should be read in conjunction with our Equal Opportunities and GDPR policies.

Statement of principle – Equality

We will take all possible steps to ensure that this policy does not discriminate, either directly or indirectly against any individual or group of individuals. When compiling, monitoring and reviewing the policy we will consider the likely impact on the promotion of all aspects of equality as described in the Equality Act 2010.

Statement of principle – GDPR

Penk Valley Academy Trust recognises the serious issues that can occur as a consequence in failing to protect an individual adult's or child's personal and sensitive data. These include emotional distress, physical safety, child protection, loss of assets, fraud and other criminal acts.

Penk Valley Academy Trust is therefore committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA)/GDPR.

Penk Valley Academy Trust will be referred to as **PVAT** for the remainder of the document which includes all schools who are members of PVAT, business operations and centralised services.

BYOD POLICY

Contents

1. Purpose
2. Policy statement
3. Future considerations
4. Conclusion

1. Purpose: This policy outlines the school's stance on the use of personal devices by students within the school premises. The primary aim is to ensure a safe and secure learning environment for all students.

2. Policy Statement: At present, the school does not permit students to bring their own devices (BYOD) for use during school hours. This decision is based on several key considerations:

Security Concerns:

- **Uncontrolled Applications:** The school currently lacks the ability to control the applications installed on personal devices. This poses a significant security risk as unauthorized or harmful apps could compromise the school's network and data. Malicious software could lead to data breaches, exposing sensitive information about students and staff.
- **Network Vulnerabilities:** Personal devices may not have the same level of security as school-provided devices. This can create vulnerabilities in the school's network, making it susceptible to cyber-attacks, malware, and other security threats.
- **Data Privacy:** Without proper controls, personal devices could inadvertently share or leak confidential information. This includes student records, personal data, and other sensitive information that must be protected under data privacy regulations.
- **Inconsistent Security Measures:** Personal devices may not adhere to the same security protocols as school devices, such as regular updates, antivirus protection, and secure configurations. This inconsistency can lead to security gaps and potential exploitation by malicious actors.

Monitoring and Management:

1. The school does not have the necessary infrastructure to monitor and manage personal devices effectively. This includes the inability to track usage, enforce security policies, and ensure compliance with the school's digital safety standards.
2. Lack of Monitoring Software: Currently, there is no monitoring software capable of overseeing the activities on personal devices. This makes it challenging to detect and prevent inappropriate use, cyberbullying, or access to harmful content.

Mobile devices:

- In line with the school's existing policy, mobile phones are generally banned during school hours to minimize distractions and promote a focused learning environment. Allowing BYOD would conflict with this policy and potentially disrupt the educational process.

3 Future Considerations: The school recognizes the potential benefits of a BYOD program and is committed to exploring this option in the future. Once the necessary infrastructure and monitoring capabilities are in place, the school will revisit this policy and consider implementing a controlled and secure BYOD program.

4 Conclusion: The school and trust remain dedicated to providing a safe and effective learning environment. We appreciate the cooperation of students and parents in adhering to this policy. Updates and changes to this policy will be communicated as the school's infrastructure evolves.