Document owner	Etwall Primary School	**Approved by:**	Headteacher – Sarah Bentley Zoe Poynton – Safeguarding Governor
Author:	Sarah Bentley	**Next Review**	September 2027
Version 1.1:	September 2026	**Signed by Headteacher**	

Bring Your Own Device

POLICY

At Etwall Primary School we believe that everyone should be included and that there is equality of opportunity for everyone, regardless of race, gender, ability, disability and social factors. This policy is intended to be inclusive of all in the school and wider school community.

ETWALL PRIMARY SCHOOL

Bring Your Own Device Policy (BYOD)

This policy has been reviewed against statutory mobile phone guidance effective from 1 September 2026 and relevant school policies.

1. Purpose and relationship with the Mobile Phone Policy

This policy governs the authorised use of personally owned laptops, tablets and other non-school devices to access the school's guest network or approved school systems. It protects pupils, staff, school information, networks and devices.

This policy does not create a right to use a personal device. Permission must be given by the school and may be withdrawn at any time. In accordance with statutory mobile phone guidance, Etwall Primary School's BYOD arrangements do not include pupil or staff mobile phones. Mobile phones and smartwatches are governed by the Mobile Phone and Smart Technology Policy. A staff phone may only access an approved school system where this is necessary for multi-factor authentication or another specifically authorised purpose, and this limited access does not make the phone part of the BYOD scheme.

2. Scope

This policy applies to staff, governors, contractors, volunteers and visitors who have been authorised to use a personally owned laptop, tablet or other permitted device to connect to the guest network or access school information. Pupils do not take part in a BYOD scheme at Etwall Primary School.

USB storage and other removable media are governed by the IT Security and Acceptable Use Policy and may only be used where expressly authorised and appropriately encrypted. Wearable communication devices and smartwatches are governed by the Mobile Phone and Smart Technology Policy and are not BYOD devices.

3. Principles

- The school will not require staff to provide or use a personal device for work.
- School-owned, managed equipment should be used wherever practicable.
- Access will follow the principle of least privilege and will be limited to approved systems and information needed for the user's role.
- School personal data must not be stored locally on a personal device or in a personal cloud account.
- The school may refuse or withdraw permission where security, safeguarding, conduct or operational concerns arise.

4. Authorisation and acceptable use

- Permission must be obtained before a personal device connects to the guest network or accesses school information.
- Users must comply with the Mobile Phone Policy, IT Security and Acceptable Use Policy, Staff Code of Conduct, Online Safety Policy and Data Protection Policy.
- Personal devices must not be used in front of pupils unless the use is expressly authorised and professionally appropriate.
- Users must not attempt to bypass filtering, monitoring, access controls or other security measures.

- Only licensed, supported and lawfully obtained software may be used.
- The guest network must not be used for illegal, offensive, discriminatory, harmful or inappropriate activity.

5. Security requirements

- The device must use a strong passcode, password or biometric lock and must auto-lock after a short period of inactivity.
- The operating system, browser, applications, anti-malware protection and security patches must be supported and kept up to date.
- Multi-factor authentication must be enabled where the approved school service supports it.
- Lock-screen notifications must not reveal school information or personal data.
- Devices must not be shared with family members or others while signed in to school services.
- Users must not save passwords in an insecure form or allow another person to use their account.
- The device must be encrypted where this is supported and required for the approved use.
- Rooted, jailbroken, unsupported or otherwise security-compromised devices must not access school systems.

6. School data and systems

- School information must be accessed through approved applications, secure web services or other methods authorised by the school.
- Personal data about pupils, families, staff or governors must not be downloaded to or intentionally stored on a personal device.
- Where a file is temporarily cached by an approved application, the user must not copy it elsewhere and must sign out when finished.
- School information must not be transferred to personal email, personal messaging services, personal cloud storage, removable media or unapproved AI systems.
- Screens must be positioned to prevent unauthorised viewing, particularly in public places.
- Users must immediately report unauthorised access, accidental disclosure or any other suspected data breach.

7. Photographs, video and audio

Personal devices must not be used to photograph, film or audio-record pupils, their work, staff, visitors, conversations or school records. There is no routine exception that allows staff to capture pupil images on a personal device and delete them later. School-owned equipment and approved school processes must be used. This includes, but is not limited to, mobile phones, smart watches and other wearable technology.

8. Network access and monitoring

Authorised personal devices may connect only to the segregated guest network unless the school's IT provider has expressly approved another secure arrangement. Access is at the school's discretion and may be suspended or withdrawn.

The school may log and monitor activity carried out through its networks and systems for security, safeguarding, compliance and service-management purposes, in accordance with its privacy information and applicable law. Monitoring does not give the school general access to unrelated personal content stored on the device.

9. Loss, theft, disposal and change of ownership

- Loss, theft or suspected compromise of a device that has accessed school systems must be reported immediately to the Headteacher, School Business Manager and Data Protection Officer.
- The user must cooperate with proportionate protective action, such as changing passwords, ending active sessions or removing school access.
- Before a device is sold, transferred, recycled, repaired or given to another person, all school accounts, applications, cached data and access tokens must be removed.
- The school is not responsible for personal devices, accessories, repairs, support, data loss, theft or damage except where liability cannot lawfully be excluded.

10. Support, inspection and privacy

The school does not provide technical support for personal devices. A user may be asked to demonstrate that required security controls are enabled or to provide limited information needed to investigate a school-system or network incident. Any inspection of personal content or the device itself must be lawful, necessary and proportionate, with advice sought where appropriate.

11. Safeguarding and professional boundaries

- Personal devices must not be used to communicate privately with pupils or to exchange personal contact details.
- Communication with parents and carers must use school-approved systems unless the Headteacher has authorised an exceptional emergency arrangement.
- Any concern about inappropriate content, contact, recording or device use must be reported immediately under safeguarding and low-level concerns procedures.
- Visitors and volunteers must follow the specific device restrictions in the Visitor Policy and Volunteer Policy.

12. Breaches

Access may be removed immediately where this policy is breached. Staff breaches may be addressed under the Staff Code of Conduct or disciplinary procedures. Safeguarding concerns, data breaches and suspected criminal activity will be referred through the appropriate procedures and to external agencies where required.

13. Monitoring and review

The Headteacher, School Business Manager, IT lead/provider and Data Protection Officer will support implementation within their respective responsibilities. The Governing Board will maintain appropriate oversight. The policy will be reviewed annually and sooner where risks, technology, law or guidance change.

Related policies and documents

- Mobile Phone and Smart Technology Policy
- IT Security and Acceptable Use Policy
- Online Safety Policy
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- AI Policy

- Visitor Management and Visitors on Site Policy
- Volunteer Policy
- Off-site Working Policy
- Educational Visits Policy

Appendix 1: BYOD authorisation record

User and role: _____

Device type and asset description: _____

Approved purpose: _____

Approved school systems: _____

Guest network access required: _____

Security controls checked by/date: _____

Authorised by/date: _____

Review or end date: _____

I confirm that I have read and will follow this policy. I understand that authorisation may be withdrawn and that school data must not be stored on my personal device.

User signature: _____ Date: _____