

Mobile Device Policy



THIS POLICY WAS AGREED BY TRUSTEES ON (Date):	August 2026
REVIEW DATE:	August 2027
CHAIR OF TRUSTEES:	
CEO:	

Contents

1. Purpose	3
2. Scope	3
3. General Principles	3
4. Pupil Mobile Device Expectations.....	4
4.1 Mobile Device-Free School Day	4
4.2 Bringing Mobile devices into School	4
5. Confiscation Procedures	4
5.1 First Breach.....	4
5.2 Second Breach	4
5.3 Repeated or Persistent Breaches	4
5.4 Curriculum Use of Mobile Device	5
6. Pupil Device Security Requirements	5
7. Staff Use of Mobile Devices	5
8. Cyber Security Requirements	6
9. Privacy, Safeguarding and Recording.....	6
10. Medical and Exceptional Circumstances	7
11. Monitoring and Compliance	7

1. Purpose

This policy aims to:

- Safeguard pupils, staff and visitors.
- Minimise distraction and disruption to learning.
- Support positive behaviour and attendance.
- Ensure compliance with safeguarding, data protection and cyber security requirements.
- Allow appropriate professional use of personal devices by staff where necessary for work purposes.
- Maintain a secure digital environment across all Trust schools.
- This policy reflects current Department for Education (DfE) expectations that schools should operate as mobile device-free environments for pupils during the school day unless a specific exception is authorised.

2. Scope

This policy applies to:

- All pupils.
- All staff.
- Agency workers.
- Volunteers.
- Governors and Trustees.
- Contractors.
- Visitors.

Mobile devices may be, but are not limited to: Mobile phones, Smartphones, Smart watches, Tablets, Personal laptops, or any device capable of communication, radio broadcast, recording, photography, internet access or data storage.

3. General Principles

Everyone bringing a mobile device onto Trust premises is responsible for ensuring that:

- The device is maintained with current operating system updates.
- Security patches are installed promptly.
- Anti-malware protection is enabled where appropriate.
- The device is protected by a password, PIN, biometric authentication or equivalent.
- The device is used in accordance with Trust/Schools safeguarding, behaviour, ICT AUP and data protection policies.

No personal device may be used in a way that:

- Compromises safeguarding.

- Circumvents Trust security controls.
- Accesses, records or monitors another person's data without permission.
- Introduces malware or security vulnerabilities.
- Disrupts learning or school operations.

4. Pupil Mobile Device Expectations

4.1 Mobile Device-Free School Day

- In line with DfE guidance, pupils must not use mobile devices at any point during the school day. This covers the time between the start of the first registration period and the end of the school day.

4.2 Bringing Mobile devices into School

Where students bring a mobile device into school for travel or safety reasons, the following directions must be followed:

- Devices must be switched off or placed in silent mode.
- Devices must remain out of sight at all times.
- Devices must not be used unless directed by a member of staff.
- The Trust accepts no liability for loss, theft or damage to personal devices.
- In primary schools – any children who bring phones into school must drop these at the school office and collect them at the end of the day (this will be individually agreed with each child)

5. Confiscation Procedures

- Where a pupil's device is: Seen, heard, used or accessed without permission, it will be confiscated and held in an agreed location within school until the end of the day.

5.1 First Breach

- Device confiscated until the end of the school day.
- Recorded on the school's behavior system.

5.2 Second Breach

- Device confiscated until collected by a parent/carer.
- Additional behavior sanctions may be applied

5.3 Repeated or Persistent Breaches

The school may:

- Require daily hand-in procedures.

- Remove permission to bring a Device onto site.
- Apply escalating behavior sanctions.
- Meet with the student and parent to discuss the breach.
- Schools retain legal powers to confiscate devices where permitted by legislation and school behaviour policies.

5.4 Curriculum Use of Mobile Device

The Trust recognises that mobile technology may occasionally support learning. Pupils may use a Device for curriculum purposes only where:

- The activity is planned by a member of staff.
- A risk assessment has been considered where necessary.
- The pupil if above the age of 13 or the parent/carer where the pupil is under 13 years old have signed the Mobile Device Learning Agreement appendix at the base of this form.
- Approval may be withdrawn at any time.

During authorised use:

- Only approved apps and websites may be accessed.
- Devices must only be used for the directed learning activity.
- Recording of individuals is prohibited unless specifically authorised.

6. Pupil Device Security Requirements

- Any pupil device brought onto Trust premises must:
- Have up-to-date operating system software.
- Be free from known malware.
- Not contain tools designed to bypass school filtering or monitoring.
- The following are prohibited:
- VPN services.
- Proxy services.
- Anonymous browsing tools intended to bypass filtering.
- Packet sniffing tools.
- Network scanning software.
- Remote access software unless explicitly approved.
- Hacking or penetration testing tools.
- Applications designed to access, monitor, intercept or collect the data of others.
- Any device suspected of compromising school systems may be removed from the network immediately and dealt with under the behaviour policy.

7. Staff Use of Mobile Devices

The Trust recognises that staff may need to use personal mobile devices for legitimate professional purposes. As such staff may use personal phones:

- For work-related communication.
- To access Trust systems where authorised.
- For safeguarding applications or processes approved by the Trust.
- During non-contact periods where appropriate.
- During staff breaks.
- Staff must ensure use remains professional, proportionate and does not detract from supervision responsibilities.

Staff must not:

- Use Devices while actively teaching unless for educational or operational purposes.
- Access personal accounts, systems or social media whilst supervising pupils.
- Photograph or record pupils using personal devices.
- Store safeguarding information on personal devices unless approved and secured.
- Use personal devices to communicate with pupils except through authorised Trust systems.
- All pupil communication must occur through approved school platforms.

8. Cyber Security Requirements

All users bringing personal devices onto site must comply with Trust cyber security arrangements.

Users must not:

- Connect unauthorised equipment to Trust infrastructure.
- Install software affecting school systems.
- Attempt to bypass filtering, monitoring or security controls.
- Share network credentials.
- Access systems beyond their authorised permissions.

The Trust reserves the right to:

- Restrict access to networks.
- Remove devices from networks.
- Investigate suspected security incidents.
- Refer serious incidents for disciplinary action.

9. Privacy, Safeguarding and Recording

Personal devices must never be used to:

- Secretly photograph, film or record others.
- Share images without consent.
- Capture confidential information.
- Access or distribute inappropriate content.
- Any safeguarding concern involving a mobile device must be reported immediately to the Designated Safeguarding Lead.

10. Medical and Exceptional Circumstances

Reasonable adjustments will be made where:

- A device supports a medical condition.
- A device forms part of an EHCP provision.
- There are safeguarding, disability or accessibility needs.
- Such arrangements must be agreed with the school and documented.

11. Monitoring and Compliance

The Trust may monitor network activity to ensure compliance with this policy, and appropriate use of mobile devices. This can result in the restriction of IT and device access.

Failure to comply with this policy may result in:

- Behaviour sanctions for pupils.
- Withdrawal of device privileges.
- Staff disciplinary procedures.