



Guidance for use of Electronic Devices 2026-27

Approved by:	Board of Trustees	Date: 27 th August 2026
Last reviewed on:	5 th August 2026	
Next review due by:	4 th August 2027	

Contents

1. Introduction	3
2. Principles	3
3. Use of mobile phones during the working day	4
4. Business use	4
5. Security.....	5
6. Text Messages.....	5
7. Social Networking	6
8.Safeguarding Employees.....	6
9. Health and safety considerations	6
10. Mobile phones and pupils.....	6
Appendix A – Acceptable use agreement	8

1. Introduction

The purpose of this guidance is to inform employees of the expectations of mobile phone use during their working hours. It is intended to give staff some broad guidelines regarding the appropriate use of mobile phones, in the workplace or in the course of carrying out your duties.

Schools are legally responsible for their own data and therefore have a duty to protect employees in relation to the use of mobile phones provided for the purposes of work.

This policy applies to all individuals who have access to personal mobile phones on site. This includes (but is not limited to) staff, volunteers parents/carers, visitors, contractors, and governors, who should be made aware of the requirements of this guidance.

2. Principles

This guidance applies to all Trust employees.

This guidance should be used in conjunction, where necessary, with the following policies:

- Social Networking Protocol
- Guidance for safer working practices for adults who work with children and young people
- Safeguarding and Child Protection Policy
- Staff Handbook
- Staff Code of conduct
- Disciplinary policy
- Lone working policy
- Lockdown policy
- Online Safety Policy.

This guidance relates to all forms of communication, including but not limited to phone and video calls, text and picture messages, emails, instant messaging and collaboration platforms.

It applies equally to:

- Mobile phones
- Tablets
- Laptops
- Smart watches
- Wearable technology
- Smart glasses (including Meta Ray-Ban and similar devices)
- AI-enabled devices
- Personal assistants and voice-activated devices
- Devices capable of recording audio, images or video
- Any device capable of storing, transmitting or processing Trust information.

The “use” of a mobile phone also includes accessing the internet for any purpose on a mobile phone as well as accessing social networking sites from your device. If an employee chooses to bring their mobile phone to work they do so entirely at their own risk.

Where the headteacher/line manager discusses mobile phone use with an employee, a record of the discussion should be kept.

Where an employee has any concerns regarding the use of mobile phones in school these should be reported to the headteacher/line manager.

Artificial Intelligence (AI)

For the purposes of this guidance, Artificial Intelligence (AI) includes generative AI technologies capable of producing text, images, video, audio, code or analysis in response to user prompts, including Trust-approved and publicly available AI tools.

3. Use of mobile phones during the working day

Employees should have their phones on silent or switched off and out of sight. All mobile phones must be kept in a secure place (e.g. in a drawer, bag) during class time.

Use of phones (including receiving/ sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms. Employees using their phones during break times should be respectful of their colleagues.

Any urgent contact should be made via the school's landline number so that a message can be relayed to the employee when they are available unless there is an emergency situation. In these circumstances, employees should make the headteacher and office aware so that there is no delay in receiving the messages. If appropriate, with prior discussion, the headteacher/line manager may grant permission to accept personal calls during work time.

Staff must not use personal devices capable of recording audio, images or video whilst undertaking duties involving pupils.

This includes:

- Mobile phones
- Smart watches
- Smart glasses
- Wearable cameras
- AI-enabled recording devices.

Recording of pupils, staff or visitors may only take place using authorised Trust equipment and for approved educational, operational or safeguarding purposes.

The use of smart glasses or wearable devices capable of covert audio or video recording is prohibited whilst carrying out duties on behalf of the Trust.

4. Business use

Any employees who have been provided with a mobile phone for business use must ensure the mobile used is solely for this reasons, unless express permission has been given that the phone can also be used for personal use.

The Trust has the authority in place to ensure that such business mobile phones and associated phone bills are checked on a regular basis.

Personal mobile phones, cameras or video recorders should not be used to record classroom activities. ONLY school equipment should be used.

Employees are discouraged from setting up their work emails on their personal mobile devices (phones, tablets etc.) in order to preserve work life balance. If employees choose to set up their work emails in this way there should not be an expectation that these emails be read, responded to or acted on outside of working hours.

Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the school office or a work mobile phone or a number will be provided as a point of contact.

In some circumstances trade union officers may need to make calls during the school day. If this is the case express permission should be sought from the headteacher

In the event of “lockdown” within the school, mobile phones should be used only in accordance with the school’s Lockdown Procedure.

5. Security

All employees have a responsibility to ensure compliance with confidentiality rules/GDPR legislation. An employee using a mobile phone at work must ensure this responsibility is maintained.

Employees choosing to access work emails using their personal mobile phones should have the appropriate secure systems in place. Employees should be requested to sign a declaration to ensure their phone is password or pin protected. (See appendix 1) This should be signed and kept on an employee’s personal file.

Employees should ensure that passwords on devices are not shared with others and should be updated/changed regularly to maintain security. Devices used to access Trust systems should, where technically possible:

- Utilise Multi-Factor Authentication (MFA)
- Be protected by a PIN, password or biometric authentication
- Maintain current software and security updates
- Have encryption enabled
- Support remote wiping facilities where Trust information is accessible.

Artificial Intelligence

Employees may only use AI tools in accordance with Trust guidance.

Employees must not:

- Input confidential information into unauthorised AI systems
- Upload personal data relating to pupils, staff, parents, governors or trustees into publicly available AI platforms
- Use AI-generated content without appropriate professional review and verification
- Create or manipulate images, audio or video involving pupils, staff or parents using AI technology unless specifically authorised
- Rely solely on AI-generated information when making professional decisions.

Employees remain personally responsible for all content submitted to, generated by or shared through AI systems.

Deepfake

Staff must not create, share, distribute or knowingly store manipulated, synthetic or AI-generated images, video or audio recordings that misrepresent pupils, staff, parents, governors, trustees or the Trust.

Any suspected deepfake, identity misuse or manipulated digital content involving members of the Trust community must be reported immediately to the Headteacher and Designated Safeguarding Lead.

6. Text Messages

Text messages are not an appropriate formal means of communicating with colleagues within a school/workplace setting as they are:

- Not a formal means of communication
- Can be misinterpreted
- Inappropriate for the purposes of audit.

7. Social Networking

Employees should not access personal social networking sites, messaging applications, AI chat platforms or similar online communication services during working hours unless authorised for educational or operational purposes.

This includes but is not limited to:

- Facebook
- Instagram
- TikTok
- Snapchat
- WhatsApp
- Telegram
- Discord
- Threads
- Generative AI platforms and similar technologies.

Where a school social networking site exists this should be set up using appropriate privacy settings and only accessed by authorised users. Access and management of these sites should not be done on personal mobile phones or devices.

8.Safeguarding Employees

Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents.

Employees should refer to the school's own policy for the use of texting/phoning parents where one exists.

Staff should never send to, or accept from colleagues, parents or pupils texts, images or links that could be considered inappropriate or which have the potential to offend.

Employees must not create, store, transmit or share images, recordings or AI-generated content involving pupils except where authorised for legitimate educational or safeguarding purposes.

Any misuse of electronic devices that creates a safeguarding concern must be reported immediately in accordance with the Trust Safeguarding and Child Protection Policy.

Any unauthorised recording of pupils, staff or visitors, whether by mobile phone, smart watch, smart glasses or other device, will be treated as a serious disciplinary matter and may result in referral to external agencies where appropriate.

9. Health and safety considerations

In circumstances where employees are lone-working in remote areas of the school, or out of hours, a work mobile or two-way radio should be provided if there is no land-line in the room.

Employees are reminded that using hand held mobile phones whilst driving is a criminal offence.

10. Mobile phones and pupils

Schools should have a separate policy which specifically covers the use of mobile phones by pupils.

Employees should be aware that there may be occasions where pupils could provoke staff to gain a particular reaction which may then be recorded.

If an employee receives material deemed to be inappropriate or offensive, the images/text messages should be retained as evidence and referred immediately to the headteacher/line manager.

Employees should remain alert to emerging technologies that may enable covert recording, communication or image capture by pupils, including smart watches, smart glasses and other wearable technology, and should report any concerns in accordance with school safeguarding procedures.

Appendix A – Acceptable use agreement

Whilst our School promotes the use of technology or devices and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the Headteacher for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

The School may undertake monitoring activities of employees to ensure the quality and quantity of work. The School will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the School will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as unintrusive as possible to the employees.

Information which is gathered from monitoring activities must have a lawful basis. The School understands rights and the private lives of workers, particularly as remote working excessive monitoring can have adverse impacts continues to become more common, that excessive monitoring can have adverse impacts on data protection rights and the private lives of workers, particularly as remote working continues to become more common.

The School will ensure that the monitoring of workers is necessary for the identified reasons. The School will also ensure that all suitable safety checks are carried out prior to monitoring activities.

Please read this agreement carefully, and sign electronically via Every Compliance to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR
- Follow the Trust's Data Protection Policy and any other relevant school policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems
- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Only use ICT systems which I have been permitted to use
- Ensure I obtain permission prior to accessing materials from unapproved sources
- Only use the internet for personal use during out-of-school hours, including break and lunch time
- Only use recommended removable media and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the Headteacher
- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities
- Only access websites and apps that have been approved by the Headteacher
- Understand that the usage of my school-owned devices will be monitored
- Keep my school-owned devices with me or within my sight at all times
- Transport school-owned devices safely
- Provide suitable care for my school-owned devices at all times
- Only communicate with pupils and parents on school-owned devices using appropriate channels
- Ensure I install and update security software on school-owned devices as directed by the Headteacher
- Seek permission from the Headteacher before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors
- Immediately report any damage or loss of my school-owned devices to the School Operations Manager
- Immediately report any security issues, such as downloading a virus, to the School Operations Manager
- I understand that if equipment is damaged on more than one occasion, the circumstances may be reviewed. Where repeated damage is found to be the result of poor care, negligence or misuse, I may be required to contribute towards repair or replacement costs, in line with Trust policies and applicable employment legislation.
- Make arrangements to return school-owned devices to the School Operations Manager upon the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the Headteacher
- Install any software onto school-owned devices unless instructed to do so by the Headteacher
- Use school-owned devices to send inappropriate messages, images, videos or other content
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content
- Use school-owned devices to access personal social media accounts

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times
- Ensure personal devices are either switched off or set to silent mode during school hours
- Only make or receive calls in specific areas, e.g. the staff room
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom
- Understand that I am liable for any loss, theft or damage to my personal devices

I will not:

- Use personal devices to communicate with pupils or parents
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the Headteacher
- Use personal devices to take photographs or videos of pupils or staff
- Store any school-related information on personal devices unless permission to do so has been given by the Headteacher.

Social media and online professionalism

I will:

- Follow the Trust Social Media Policy
- Understand that I am representing the school and behave appropriately when posting on school social media accounts
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels

Working from home

I will:

- Ensure I obtain permission from the Chief Finance and Operations Officer before any personal data is transferred from a school-owned device to a personal device
- Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted
- Ensure my personal device has been assessed for security by the ICT technician before it is used for home

- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety
- Allow the Headteacher and School Operations Manager to undertake regular audits to identify any areas of need I may have in relation to training
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices
- Deliver any training to pupils as required.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the Headteacher
- Understand that my use of the internet will be monitored by the ICT technician and recognise the consequences if I breach the terms of this agreement
- Understand that the Headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

Monitoring workers

I understand that:

- The school will notify employees when monitoring takes place and that the school will clearly explain what personal information of mine is collected and how it's utilised and maintained
- Monitoring is often used for security purposes, managing employees' performance, and monitoring sickness and attendance
- Monitoring technologies include, but aren't limited to, camera surveillance, webcams, technologies for timekeeping and keyboard activity, productivity tools, internet activity trackers, body-worn devices, and hidden audio recording
- Personal data relating to myself which is collected from monitoring activities is securely kept and protected and isn't kept for any longer than necessary by the school
- The school will factor in increased expectations of privacy if I work from home
- The school will conduct its monitoring activities in a way that's fair and reasonably expected
- The school will conduct its monitoring activities with transparency, clearly explaining how and why they process my information
- The school will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR
- I can object to having my personal information collected and processed if the lawful basis which the school is relying on is a public task or legitimate interests based on my personal situation
- The school may refuse to comply with the objection if they can demonstrate that the monitoring is for legitimate interests which override my interests, rights, and freedoms, or that the monitoring is for establishment, exercise, or defence of legal claims

- Tools for monitoring workers continue to become increasingly sophisticated, and that the school will inform me if they choose to use solely automated processes for monitoring activities
- I can access the information collected by the school by making a subject access request (SAR)
- The school will carry out a data protection impact assessment (DPIA) prior to undertaking their monitoring activities. Completing a DPIA identifies and minimises any potential risks that come with monitoring activities.