Digital Devices Policy

'We seek to ensure that all our children learn and thrive in an environment completely free from the fear of intimidation by others.'

Reviewed September 2026

Next Review due September 2027

Contents

1. Definition of terms used in the policy
2. Policy overview
3. Relevant Legislation and Guidance
4. Roles and Responsibilities
5. Use of mobile phones by staff and volunteers, including directors and governors
6. Use of mobile phones by pupils
7. Use of mobile phones by parents/carers and other visitors
8. Use of Photography and Images
9. Use of Social Media

1. Definitions

For the purpose of this policy, the following definitions are used

Mobile phone - phones and any other device capable of recording, messaging, calling or accessing the internet, including smart watches, other wearables and tablets.

Social media - all technologies that allow individuals to communicate and share information (including photos and video). This includes specific applications such as Facebook, X, Instagram, Threads etc. but also, games, for example Minecraft, Roblox, Fortnight, and video sharing platforms such as You Tube which have social media elements to them. The policy also applies to personal web pages, personal space provided by internet providers and any other internet presences which make available personal information (including images) and opinions to the general public.

Photography and Images – includes videography and covers images captured as digital files by cameras and mobile phones and by analogue devices.

Personal Communications - those made via a personal social media or other personal account

Professional Communications - those made through official channels, posted on a Trust or school account, or using the Trust or school name.

contents

2. Policy Overview

As a Trust, with members which are Church of England Schools, this policy reflects the Christian values of honesty, compassion, respect, and encouragement. We seek to ensure that all our children learn and thrive in an environment completely free from the fear of intimidation by others.

The purpose of this policy is to:

- Protect pupils from harm linked to mobile, smart, digital and photographic technology
- Maintain high standards of behaviour and focus for learning

- Provide clear expectations for staff, directors, governors, volunteers, pupils, parents and visitors
- Reduce risks associated with recording, messaging, internet access and social media
- Ensure professional conduct and safeguarding compliance

- contents

3. Relevant Legislation and Guidance

This policy is based on legislation and advice from the Department for Education (DfE) on:

- Mobile Phones in Schools 2026
- Behaviour in schools: advice for headteachers and school staff 2024
- Searching, screening and confiscation: advice for schools 2022
- Keeping Children Safe in Education 2026
- UK General Data Protection Regulations
- Data Protection Act 2018
- The Data (Use and Access) Act 2025
- Human Rights Act 1998

The policy should be read in conjunction with the following related policies

- Child Protection and Safeguarding Policy
- Staff and Governance Codes of Conduct
- School Behaviour Policy
- Acceptable use agreements

- contents

4. Roles and Responsibilities

- Staff are responsible for complying with and consistently enforcing this policy.
- Volunteers are responsible for complying with this policy and to alerting a member of staff if they witness, or aware of a breach of the policy.
- Directors are responsible for ensuring that the policy is regularly reviewed and for complying with the policy
- Governors are responsible for complying with this policy and monitoring compliance within their school.

- Parents/carers are responsible for complying with this policy and supporting compliance by their children
- Pupils are responsible for complying with this policy.

It is expected that all schools will have at least one wireless internet network (Wi-Fi). Any staff devices that are not supplied directly by the Trust should only access the guest Wi-Fi network

contents

5. Use of mobile phones by staff and volunteers, including directors and governors

5.1 Personal Phones

- Staff and volunteers are not permitted to use their personal mobile phone for personal business while children are present.
- Use is defined as making or receiving calls or personal messages, accessing social media or notifications
- Personal phones and other devices may only be connected to the premises' guest wireless internet network.
- Phones must be on silent (or switched off) and stored out of sight during the school day.
- Use is only permitted during staff non-contact time in staff-only areas

Emergency messages should ordinarily be directed via the school office. Where staff need access to their phone due to a specific personal circumstance (e.g. medical need, or urgent family situation), this must be agreed in advance with the Headteacher or line manager.

5.2 Phones for work purposes

While some members of staff are provided with a mobile phone by the Trust or its schools for work purposes, others with a community contact role such as Designated

Safeguarding Leads (DSLs), Parent and Family Support Advisers (PFSAs) and Senior Leaders may be required to use their personal phones for work purposes.

Staff must:

- As far as is practicable, avoid the use of mobile phones in the presence of children.
- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with the staff code of conduct
- Secure the device with a password, PIN or biometric lock
- Ensure notifications are not visible to pupils

Only authorised staff are permitted to use Trust/school phones, and access to the phone must not be provided to anyone without authorisation. Any misuse should be reported immediately.

- contents

6. Use of Mobile Phones by Pupils

Schools are required to publish details of their policy on the use of mobile phones. PPAT schools may choose to draw parents' attention to this annex when sharing the Child Protection policy, adapt sections 6 and 7 as a standalone document or adapt section 6 as part of their behaviour or on-line safety policy.

6.1 During the school day

The Trust has adopted a "not seen, not heard, not used" approach to the use of mobile phones by pupils during the school day. This includes before school, during lessons, in the times between lessons, at break/lunch times and during enrichment activities. If parents need to contact their child during the school day; messages should be directed via the school office.

The term mobile phone includes phones and any other device capable of recording, messaging, calling or accessing the internet, including smart watches, other wearables and tablets.

The Trust recommends that pupils do not bring a mobile phone to school at all but recognises that some pupils who travel independently to and from school may need a phone for safety. In such cases:

- Written permission from parents/carers must be provided
- Phones must be switched off on arrival
- Phones must be handed in for secure storage
- A record of devices handed in will be kept
- Devices remain the pupil's responsibility; the Trust accepts no liability for loss or damage

Phones must not be used on school trips, visits or residentials unless explicitly authorised by the school.

Schools may permit pupils to use a mobile phone in school, due to exceptional circumstances, these will be considered on a case-by-case basis. To request such permission, parents/carers should contact the Headteacher.

If any pupil uses a mobile phone in breach of this policy:

- The device will be confiscated and stored securely
- Parents/carers will be required to collect the device
- Permission to bring a phone to school may be withdrawn
- Behaviour sanctions may be applied in line with the schools' Behaviour Policies

Smart watches are permitted at the discretion of the Head Teacher. These will be checked for capabilities such as online access, camera, messaging etc. If the Head deems the watch to be used exclusively for the process of telling the time and the pupil understands this, it will be permitted. No wearables with a camera will be permitted.

6.2 Outside of the school day

In line with DfE behaviour guidance, the Trust reserves the right to act where mobile phone use outside school:

- Leads to bullying, intimidation or harassment of pupils or staff
- Causes disruption or safeguarding concerns within schools
- Involves inappropriate images, messages or online conduct

Senior leaders may search a pupil's device, where lawful and reasonable, if there is suspicion it contains:

- Indecent images
- Evidence of bullying or harassment
- Material relating to a criminal offence or safeguarding concern

Serious incidents may involve external agencies, including the police. Examples of serious misuse include:

- Sharing indecent images (sexting)
- Online threats or harassment
- Discriminatory or abusive messages
- Filming or photographing others without consent

contents

7. Use of mobile phones by parents/carers and other visitors

The Trust recognises that mobile phones are an essential part of modern life, but for reasons of safeguarding, all visitors are required to

- Keep their mobile phone on silent/vibrate while on Trust schools' grounds
- Use the school office as the point of contact should they need to get in touch with their child during the day

Visitors should not:

- Use phones where pupils are present or where pupils have access

- Use their phones or other devices to take photographs or recordings of pupils or staff

Parent/carers may take photographs of their own child at public events such as a school fair, performances or sports day provided that:

- The photographs and recordings are for personal use only
- No images capturing other children are shared online without express consent

Please note commercial copyright in a dramatic performance or musical will normally exclude any audio or video recording by the public. Schools should check the full licensing details prior to any performance. In the event of copyright limitations, parents and their guests will be informed that recording is forbidden. Parental photography must not include any child whose parent has refused consent for any reason. This may necessitate the school offering photography opportunities before or after the event of those who are authorised to be involved and restricting all other recording

8. Use of photography and images

Photography and videography in schools is subject to the Data Protection Act 2018 regarding the rights of individuals to have information of a personal nature treated in an appropriate manner and the Human Rights Act 1998, protecting the privacy of individuals and families.
As well as these statutory rights, restrictions on photography arise from issues of safe guarding and copyright in performances.

contents

8.1 Use by the Trust

Photographs of Children

There are occasions when the Trust may wish to capture video or photographs of pupils at its schools. This may be for educational purposes or for use on its websites, in printed materials and social media. The written permission of parents/carers will always be sought and those who do not wish for their children's images to be used in these capacities, for any reason, may state this on the consent form.

If there is a disagreement over consent, or if a parent does not respond to a consent request, it will be treated as if consent has not been given and photos and videos will not be taken or published of the pupil without consent.

All parents will be entitled to withdraw or change their consent at any time during the school year. Parents who wish to withdraw their consent must notify the school in writing.

Where parents have opted out, the Trust will take steps to ensure their child's image is not identifiable in any of its materials.

For educational Aims

Staff are allowed to take digital/video images, to support educational aims

- Photographs taken by staff on school visits may be used in the curriculum and displayed within the school or at parents' evenings to illustrate the work of the school except in cases where the parent/carer has opted their child out.
- Copyright and use of photographs is carefully controlled by and retained safely by the school and by PPAT.
- Photographs held by the school must be annotated with the date on which they were taken and stored securely.
- Photographs taken for internal classroom curricular, assessment, security, registration, training and development or travel reasons will not be used for other purposes.
- When photographs are no longer needed for educational purposes, they must be deleted including from any residual or cloud attached storage that may keep a record of the image following the deletion on a local device.
- It is best practice for staff to delete images immediately following their transfer to a secure school platform and to do so with another member of staff present to verify the deletion.

Early Years Foundation Stage (EYFS)

- Photographs will be taken during indoor and outdoor play for display in albums or development records for parents to look through
- Other children may be visible in the background
- Public events, such as sports day, may also be recorded by both staff.

Promotional Materials

The Trust may wish to capture video or photographs of pupils at its schools for use on its websites, in printed materials and social media. The written permission of parents/carers will always be sought and those who do not wish for their children's images to be used in this capacity, for any reason, may state this on the consent form.

Where parents have opted out, the Trust will take steps to ensure their child's image is not identifiable in any of its materials.

The Trust will follow the UK Safer Internet Centre's guidance on image guidance for education settings.
Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

8.2 Photography by and of School Staff

Photographs by and of staff members may be used by the schools and in PPAT promotional materials. Staff members also have the right to opt out of these uses but must inform the schools Head teacher in writing.

8.3 Photographs by other Authorised Agencies

The involvement of other agencies can only be authorised by the Head teacher or CEO. Other agencies may include:

- Reputable commercial photographers. The law allows them to retain the copyright of the photographs they take. This applies to class or group photographs; parents will receive the contact details of the agency used for these photographs
- The press and other media. Copyright rests with the photographer.

8.4 Photography by Parents/carers

Parent/carers may take photographs/recordings of their own child at public events such as a school fair, performances or sports day provided that:

- The photographs and recordings are for personal use only
- No images capturing other children are shared online without express consent
- No copyright is infringed
- There is no interference with opportunities for other pupils' participation in the event or any effect on the health and safety of pupils and others

8.5 Photography by pupils

Pupils are not expected to have or use phones for any purpose. There may however be isolated occasions where a pupil's personal device may be permitted at the expressed permission of the headteacher such as an end of year photograph. It is good practice to record such incidents as the trust's position remains clear that these are the exception to the rule that no pupil is expected to have or to use a phone for school purposes.

On occasions when mobile phones are permitted, Pupils may wish to photograph each other. Staff will:

- Maintain the supervision and management control expected in their "duty of care" role
- Educate pupils about acceptable behaviour when photographing peers
- Confiscate the devices of pupils who do not follow instructions and secure them securely until they can be handed over to parents.

contents

9. Use of Social Media

PPAT respects privacy and understands that staff, volunteers, and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards of the Trust and its schools or on their reputation are within the scope of this policy. In all cases, where any personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with

an appropriate disclaimer. Such personal communications are within the scope of this policy.

Staff must not link their own sites to the Trust or to their school's website or use the Trust's or their school's or any other identifiers on their personal web pages.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

All professional communications are within the scope of this policy.

Digital communications with pupils are also under regular consideration. If PPAT decides to implement individual school social media accounts in the future, staff will be permitted to use this to communicate with learners for teaching and learning purposes but must consider whether this is appropriate and understand the potential implications of doing so.

Process for creating social media accounts.

The Trust community is encouraged to consider if a social media account will help them in their work. Anyone wishing to create such an account must present a business case to their School Senior Leadership Team (SLT) or, in the case of the central team, to the Chief Executive Officer, which covers the following points:

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Who will be able to contribute content to the account
- Will the account be open or private/closed?

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the Trust or school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the Trust or school, including volunteers or parents.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- In the event of any offensive or inappropriate comments being made, the school will ask the person responsible to remove the post and invite them to discuss the issues in person.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be always professional and respectful and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Staff must not 'friend', 'follow' or otherwise contact pupils through their personal social media accounts. If pupils attempt to 'friend' or 'follow' a staff member, they will report this to the Designated Safeguarding Lead.
- Staff and volunteers should report any pupil-initiated communication with their personal accounts to the Designated Safeguarding Lead.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be

considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff and escalated, where appropriate, under the Trust Disciplinary Policy.

- Conduct that raises safeguarding concerns will be reported to the local authority designated officer (LADO).
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.
- If a journalist makes contact about posts made using social media, staff must follow this policy before responding.

Handling abuse

- When acting on behalf of the Trust or its schools, manage offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, Trust and school users should block, report, or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging

- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook, WhatsApp, Instagram and TikTok)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with this policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Safeguarding

- Any disclosures made by pupils to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.
- Concerns regarding a staff member's online behaviour will be reported to the headteacher or CEO, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it will be reported to the chair of governors.
- Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

- Where there is a concern that illegal activity has taken place, the headteacher will contact the police. The Trust will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.
- As part of the usual communication with parents, the school will reinforce the importance of pupils being safe online and inform parents what systems the school uses to filter and monitor online use. The school will also make it clear to parents what their children are being asked to do online for school. including what platforms, they will be asked to access and who from the school, if anyone, they will be interacting with online.

Appendix A

Managing your personal use of social media and the internet:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Remember the Keeping Children Safe in Education guidance suggests that schools and colleges might want to consider an online search as part of their due diligence of shortlisted candidates.
- Know how to report a problem.

Managing school social media accounts

- Don't make comments, post content or link to materials that will bring the school into disrepute.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed, or add potentially inappropriate content.
- Don't post derogatory, defamatory, offensive, harassing, or discriminatory content.
- Don't use social media to air internal grievances.