Barham Church of England Primary School

Mobile Technology and Social Media Policy

Reviewed	**April 2026**
Date of next review	**April 2027**

Our Vision Statement

Barham is a vibrant, inclusive and high-achieving primary school with a family feel at the heart of the local and church community. We are committed to supporting each child to be confident, kind and curious. Our curriculum is broad, engaging and supports everyone to flourish as God intends.

Barham CE Primary School
Mobile Technology & Social Media Policy

Key details

- Designated Safeguarding Lead: Jo Duhig, Headteacher
- Deputy DSL: Michelle Anderson, Deputy Headteacher
- Named Governors with lead responsibility: Victoria Bruce & Tim Hopthrow

1. Policy aims and scope
   This policy safeguards and promotes the welfare of all members of the Barham School community when using mobile devices, smart technology and social media. It applies to all on-site and school-related use of devices including mobile phones, tablets, e-readers, games consoles, and wearable technology (for example smartwatches) that facilitate communication or have the capability to record sound or images.

This policy supports the school's statutory duties as set out in Keeping Children Safe in Education (DfE, 2025) and the DfE Filtering & Monitoring Standards for Schools and Colleges. It should be read alongside the school's Child Protection Policy, Online Safety Policy, Data Protection Policy and Acceptable Use Policies.

2. Links with other policies
   This policy should be read in conjunction with:
   - Child Protection Policy
   - Acceptable Use Policy (AUP) / Remote Learning AUP
   - Behaviour & Discipline Policy
   - Searching, Screening & Confiscation Policy
   - Data Protection Policy and image use procedures
   - Anti-bullying Policy
   - PSHE/Computing curriculum documentation
   - Staff Code of Conduct / Allegations Policy
3. Roles and responsibilities
   - The Headteacher (Jo Duhig) has overall responsibility for this policy and for ensuring it is implemented.
   - The DSL (Jo Duhig) has overall responsibility for online safety and for documenting and acting on filtering and monitoring reports; the DSL will report termly to governors on online safety and technical controls.
   - The Deputy DSL (Michelle Anderson) supports the DSL with day-to-day responses to online safety incidents.
   - The governing body receives assurance that the school meets DfE filtering & monitoring standards and receives termly summaries of online safety incidents and training.
   - Staff, learners, parents/carers and visitors must follow this policy.
4. Safe use of mobile and smart technology — general expectations
   - Personal devices brought onto site are the responsibility of the user and must be used in line with this policy and the AUP. The school accepts no responsibility for loss, theft or damage to personal devices.
   - Devices are not permitted in specific areas such as toilets, changing rooms and swimming pool areas.
   - The sending of abusive, harassing or inappropriate messages or images is forbidden and will be dealt with under behaviour/child protection procedures.

- All users must ensure their devices do not contain content that is illegal, offensive or which would contravene school behaviour or safeguarding policies.

5. School-provided devices and remote learning
    - Staff providing formal remote learning must use school-provided equipment and approved platforms in line with the Remote Learning AUP.
    - School devices are protected with passcodes/passwords and must only be used by authorised users.
    - Activity on school devices may be monitored for safeguarding and policy compliance.
6. Staff use of personal devices
    - Staff must not use personal devices to contact pupils or parents/carers. Any pre-existing relationships that make this difficult must be discussed with the Headteacher/DSL and recorded.
    - Staff should keep personal devices stored and on silent during teaching time. Personal device use in lesson time is only permitted in exceptional circumstances with SLT agreement.
    - Photographs or videos of pupils must ONLY be taken using school devices or with prior, specific written permission and in accordance with the school's image use and data protection procedures.
    - If staff need to use a personal device for school business in exceptional circumstances, written approval from SLT is required and a risk assessment must be completed.
7. Learners' use of devices
    - Pupils must not bring mobile devices to school
    - If a parent wishes their child to bring a mobile phone or personal device on site they must have prior written agreement with the Headteacher (for example medical monitoring). If permitted, devices must be handed in at the office at the start of the day, switched off and stored securely; they can be collected at the end of the school day.
    - If a learner needs to contact a parent/carer during the school day, a member of staff will provide access to a school phone.
    - Devices must not be taken into examinations. Possession of a device that facilitates communication during an exam will be reported to the awarding body and may result in withdrawal from that examination.
8. Confiscation, searching and handling of concerns
    - Staff may confiscate a device suspected of breaching this policy. Searches and examination of devices will be conducted in line with the school's Searching, Screening & Confiscation policy and KCSIE guidance.
    - Confiscated devices will be stored securely and returned to parents/carers at the end of the day unless retention is required for safeguarding reasons or police investigation.
    - If illegal material is suspected, the device will be handed to the police. LADO and other agencies will be informed as required by relevant policies.
9. Visitors and contractors
    - Visitors must follow school signage and reception guidance on device use. Personal devices are not permitted to be used in classrooms or where children are present unless approved for multi-agency work and supervised.
    - Staff must challenge visitors where concerns arise and report breaches to the DSL/SLT.
10. Social media expectations

- Staff must behave professionally online and should not use personal social media accounts to contact pupils or parents. Staff are advised not to identify themselves as employees of the school on personal accounts.
- Any online conduct that brings the school or profession into disrepute may lead to disciplinary action.
- Pupils will be taught safe, respectful use of social media through the PSHE/Computing curriculum and parents will be informed about age restrictions for services and tools.

11. Filtering and monitoring
    - The school implements appropriate filtering and monitoring in line with DfE standards. The system covers school-managed devices and, where technically possible, school-managed devices used off-site.
    - The DSL documents the arrangements for filtering and monitoring, receives reports, and acts on identified concerns following safeguarding procedures.
12. Training, communication and parental engagement
    - Online safety training is provided at induction and at least annually for all staff.
    - Pupils receive age-appropriate online safety education through the curriculum.
    - The school communicates expectations to parents/carers and provides guidance to support safe device use at home.
13. Responding to incidents and post-incident review
    - All concerns must be reported to the DSL. Safeguarding incidents are handled per the Child Protection Policy. Non-safeguarding policy breaches are managed through behaviour or staff disciplinary procedures.
    - After significant incidents, SLT and the DSL will debrief, record lessons learned and update policies or training as required.
14. Monitoring and review
    - This policy will be reviewed at least annually and whenever statutory guidance or local circumstances change.
    - The governing body will receive termly assurance from the DSL regarding compliance with DfE filtering & monitoring standards and an annual summary of online safety incidents and training.

Data protection and consent

- Parental consent for use of images will be obtained and recorded. Images must be stored using approved school systems and handled in accordance with the Data Protection Policy.
- Retention and deletion of images follows the school's data retention schedule.

Complaints and escalation

- Complaints about policy implementation should follow the school's complaints procedure. Staff are reminded of the whistleblowing procedure for raising concerns about colleagues.