Abbey Church of England Infant and Nursery School — E-Safety / Online Safety Policy

Date: 29 September 2026
Review: annual (or sooner if new statutory guidance, a safeguarding incident or significant change in technology)

Note: This document replaces the July 2024 E-Safety Policy. It reflects current statutory expectations in Keeping Children Safe in Education (KCSIE) and the Early Years Foundation Stage (EYFS) statutory framework, and aligns with DfE/NCSC guidance on cyber security and online safety.

1. Purpose and scope

This policy sets out how Abbey C of E Infant and Nursery School protects pupils and staff in their use of technology, both on and off site, and how we meet our statutory duties to safeguard pupils online. It covers:

- pupils (including those in the Early Years),
- all staff, governors and volunteers,
- school-owned devices, networks and cloud services,
- use of personal devices where they connect to or are used for school business or contact with pupils.

This policy is part of our Safeguarding suite and should be read alongside: Child Protection/Safeguarding Policy, Staff Code of Conduct (including low-level concerns), Data Protection Policy, Behaviour Policy and EYFS welfare requirements.

2. Roles and responsibilities (key points)

Headteacher (Rachel Horton): overall responsibility for online safety and is the school's e-Safety Coordinator. Ensures policy implementation, incident response and reporting to governors and local safeguarding partners where required.

Designated Safeguarding Lead (DSL) and deputies: manage online safeguarding concerns, make referrals to children's social care or police where necessary, ensure records are kept.

Safeguarding governor: monitors online safety arrangements and receives regular updates from the Headteacher (at least termly).

Computing lead / subject leader: curriculum delivery for online safety, resources for staff, supports risk assessments for technologies.

All staff: required to read, understand and follow this policy; complete induction and regular safeguarding/online safety training; report concerns or incidents immediately to the DSL.

Pupils and parents/carers: expected to follow the Acceptable Use Policy (AUP). Parents are informed about online safety and asked for consent where needed (e.g. images).

Governors retain strategic oversight and must ensure schools meet statutory duties including appropriate filtering and monitoring, staff training and annual review of online safety provision.

3. Statutory and regulatory requirements (summary)

We follow statutory guidance in:

- Keeping Children Safe in Education (KCSIE) — online safety, filtering & monitoring, staff training, continuous vigilance (statutory).
- Early Years Foundation Stage (EYFS) — safeguarding requirements for early years practitioners.
- Data Protection Act 2018 and UK GDPR — processing and storage of personal data.
  We also implement proportionate cyber security measures in line with DfE/NCSC guidance and the Cyber security standards for schools and colleges.

(Sources for these documents are listed at the end.)

4. Education and curriculum

Online safety is taught through the computing curriculum and reinforced in PSHE, assemblies and other curriculum areas. Content is age-appropriate and reflects the needs of our pupils (Nursery–Year 2), recognising high proportions of EAL and SEND in our community.

In EYFS and KS1, internet access is by adult demonstration; children are taught the Zip it, Block it, Flag it rules and simple, concrete actions to keep themselves safe online.

Learning outcomes: pupils will understand basic personal information safety, what to do if they see something that worries them and how to behave respectfully online.

Staff model safe, professional online behaviour and use resources adapted for infants (visual prompts, stories, teacher-led activities).

5. Staff training and induction

All staff (including volunteers and governors) receive safeguarding and online safety training at induction that includes expectations for filtering, monitoring, acceptable use and how to report concerns. This training is updated regularly and at least annually, and when guidance changes.

Staff receive regular updates (termly briefings) about emerging risks, low-level concerns reporting and changes to filtering/monitoring.

Staff contributing to safeguarding arrangements (DSLs, computing lead) receive enhanced training and opportunities to shape online safety practice.

6. Acceptable Use and professional conduct

All users must sign the Acceptable Use Policy before being given access to school ICT resources. Class logins are used under direct supervision.

Staff must follow the Staff Code of Conduct: use school accounts and devices for professional communications, not use personal devices to take photos of pupils, store images only on school systems and delete them when no longer needed.

Personal devices: staff must store personal mobiles and smart watches out of reach during working hours and only use them in staff-only areas at break times. Visitors may use guest logins only with permission.

7. Filtering, monitoring and cyber security

The school implements appropriate filtering and monitoring on school devices and networks. We work with Warwickshire ICT Development Service and external providers; filtering and monitoring settings are reviewed regularly by senior staff.

We carry out an annual online safety risk assessment and use UKCIS/DfE self-review tools to inform actions.

Cyber security measures (antivirus, patching, MFA where possible, secure configurations, encrypted devices and secure transfer of data) are in place in line with DfE/NCSC expectations. The school will follow the DfE Cyber Security Hub guidance and report significant incidents to the Local Authority and NCSC as required.

8. Managing incidents and reporting

All online safety incidents, including suspected child protection concerns, must be reported immediately to the DSL using the school's safeguarding reporting arrangements.

The DSL will record incidents, decide actions, escalate to statutory agencies if necessary and inform governors and the LA where appropriate. Incidents involving criminal activity will be reported to police.

The school will keep an incidents log (dates, systems/devices involved, action taken, referrals) and use learning from incidents to update policies and training.

9. Remote learning and off-site use

Remote learning provision uses approved platforms and school accounts. Staff will follow usual professional expectations for communications and live lessons; parents/carers will be given guidance.

Pupils and families will be given clear, simple instructions on safe use of any platforms and taught how to report concerns.

10. Photographs, videos and publishing pupil information

Written consent from parents/carers is obtained before publishing pupil images or work online. No pupil full names are published alongside images and images should be obscured so as to ensure anonymity.

Staff images are not published without consent. School contact details on the website are limited to the school address, general phone and office email.

Pupil work or images removed at a parent's request will be removed from public view within an agreed timeframe.

11. Social media and personal publishing

Use of social networking sites by pupils is discouraged for primary-aged children; parents will be advised of age-appropriate use.

Staff must not follow or befriend pupils on personal social media accounts. Professional use of social media must comply with the Staff Code of Conduct.

12. EYFS-specific arrangements

A designated practitioner (DSL) carries lead responsibility for safeguarding in the EYFS and liaises with local statutory partners as required.

Mobile phones and personal devices are not used to take photos in EYFS. Photographs of young children are stored on secure school systems and subject to the same parental consent arrangements.

Online safety education for early years focuses on understanding what is private, identifying trusted adults and basic reporting language for children (e.g. “I must tell an adult if…”).

13. Data protection and privacy

All processing of personal data follows UK GDPR and the Data Protection Act 2018. Staff must use secure, password-protected devices and encrypted transfer where required.

The separate Data Protection Policy sets out retention periods, access rights and data breach procedures. Any data breach must be reported immediately to the Data Protection Lead and, if required, to the Information Commissioner’s Office.

14. Monitoring, review and governance

The e-Safety Policy is reviewed at least annually by the Headteacher in consultation with DSLs, computing lead and safeguarding governor.

The governing body receives termly reports on online safety incidents, training compliance, filtering/monitoring reviews, and the annual online safety risk assessment.

The school will use UKCIS/Government self-review tools and NCSC guidance to check compliance and identify improvements.

15. Links with other policies

This policy should be read alongside:

- Child Protection/Safeguarding Policy
- Staff Code of Conduct / Low-level Concerns Policy
- Data Protection Policy
- Behaviour Policy
- Acceptable Use Policies (pupils, staff, visitors)

- EYFS statutory framework (safeguarding/welfare requirements)

16. Practical quick actions for staff (summary)

- Report safeguarding/online concerns to the DSL immediately.
- Do not use personal devices to photograph pupils; use school equipment only.
- Keep passwords private; log out of devices when not in use.
- Remind children to follow Zip it, Block it, Flag it and report anything worrying.
- If you discover an unsuitable site, log the URL, time, date and inform the computing lead/Headteacher.
