Online Safety Policy

St Agnes C of E Primary School

Approved by:	Sue Gittins
Last reviewed on:	September 2026
Next review due by:	September 2027

Online Safety Policy

Mission Statement

'Learning together in God's Love'

Our Christian Vision

St Agnes is an inclusive Christian family, we want our children to:

- Learn together with respect, patience and kindness
- **Treat each other as they would like to be treated (Matthew 7v12)**
- Flourish in education and friendships
- **Live life in all its fullness (John 10v10)**
- Be proud of themselves and others
- Ensure everyone is treated equally

Through the range of experiences we offer to all our pupils we encourage an understanding of the meaning and importance of faith and promote all the Christian Values. We particularly focus on Responsibility, Creativity, Forgiveness, Perseverance, Hope, Thankfulness and Friendship. These Christian values form the basis of our vision and are embedded throughout our school life and underpin all our teaching.

St Agnes is a small school that supports our community by providing an education of the highest quality within the context of Christian belief and practice. We work closely with our families to ensure they are fully supported and cared for.
We expect everyone at St Agnes C of E Voluntary Aided Primary School to follow 'The Great Expectations' –

Be Safe
Be in the right place at the right time
Do your best
Handle your emotions
Use appropriate language
Cooperate
Respect everyone and everything

1. Introduction

The Online Safety Policy at St Agnes C of E Primary School sets out how the school safeguards pupils, staff, governors, volunteers and visitors when digital technology, online services and connected devices are used for teaching, learning, communication or school business. Online safety is treated as an integral part of safeguarding and not as a separate technical issue.

This policy has been reviewed for September 2026 and should be read alongside the school's Safeguarding and Child Protection Policy, Behaviour Policy, Computing and Acceptable Use Policy, Artificial Intelligence Policy, Filtering & Monitoring Policy, Data Protection Policy, Staff and Governor Social Media, Messaging & Online Conduct Policy.

The policy takes account of Keeping Children Safe in Education 2026, the Department for Education digital and technology standards (including filtering and monitoring and cyber security), the revised statutory Relationships Education, Relationships and Sex Education and Health Education guidance for September 2026, the statutory Mobile Phones in Schools guidance, UKCIS Education for a Connected World and relevant data protection requirements.

2. Purpose

The school aims to:

- protect pupils and staff from illegal, inappropriate and potentially harmful online content, contact and behaviour;
- teach pupils the knowledge, critical thinking and practical skills needed to use technology safely, responsibly and respectfully;
- ensure pupils know how and where to report online concerns and that they will be listened to and supported;
- maintain proportionate filtering, monitoring, supervision and security arrangements without unreasonably restricting teaching and learning;
- set clear expectations for school-managed and personal devices, including mobile phones, smartwatches, hotspots and other connected technology; and
- respond consistently to online safety incidents, including safeguarding, cyber security and data protection concerns.

3. Online safety risks

The school considers online safety through the four broad areas of risk commonly described as the "4 Cs":

- **Content:** being exposed to illegal, inappropriate or harmful content, including violent or sexual content, pornography, misinformation or disinformation, harmful challenges, extremist material, self-harm content, deepfakes and AI-generated or manipulated material.
- **Contact:** being subjected to harmful online interaction with other users, or generative AI applications that simulate such interaction, including peer pressure, bullying, grooming, exploitation, coercion, harassment, impersonation or contact from unknown adults or children.
- **Conduct:** personal online behaviour that increases the likelihood of harm, including cyberbullying, sharing personal information, image-based abuse, making/sending/receiving nude or semi-nude images, using AI to create harmful or intimate images, or engaging in illegal or risky online activity.
- **Commerce:** risks such as scams, phishing, fraud, inappropriate advertising, in-app purchasing, gambling-style features, financial exploitation and other commercial pressure.

Risk is considered in light of each pupil's age, developmental stage, SEND, communication needs, vulnerabilities and individual circumstances. Online harms can occur both in and outside school and may overlap with child-on-child abuse, sexual harassment, exploitation, radicalisation, bullying and mental health concerns.

4. Online safety education

- Online safety is taught through Computing, Relationships and Health Education/RSHE, PSHE and other curriculum opportunities, with learning revisited and developed from EYFS to Key Stage 2.
- Teaching is age and stage appropriate and includes safe online relationships, privacy, consent and boundaries, managing personal information, recognising harmful content and contact, reporting concerns, digital reputation, cyberbullying, scams, misinformation/disinformation, AI-generated content and the fact that online material may be manipulated or misleading.

- Pupils are taught that online and offline standards of respect and behaviour are the same, and that they should seek help from a trusted adult if anything online makes them worried, uncomfortable or unsafe.
- Current issues may be reinforced through assemblies, workshops and targeted teaching where this is appropriate and does not inadvertently increase risk or exposure.
- The school provides parents and carers with appropriate information and signposting to support safe technology use at home, including emerging online risks and changes to popular platforms or devices.

5. Roles and responsibilities

- **Governing Body:** has overall strategic responsibility for safeguarding, including appropriate online safety, filtering and monitoring arrangements. Governors receive assurance that these arrangements are reviewed at least once every academic year and that identified actions are followed up.
- **Headteacher and DSL:** ensure online safety is embedded in safeguarding practice; respond to safeguarding concerns; make sure staff understand reporting routes; and work with the Digital Lead/IT support on risks arising from new technology, remote access, BYOD and generative AI.
- **SLT Digital Lead / IT Support:** support the secure operation of school technology, filtering and monitoring systems, user access, cyber security and technical controls; provide assurance that controls continue to operate following system or device changes; and escalate safeguarding concerns promptly to the DSL.
- **Computing Coordinator:** ensures that online safety education is appropriately sequenced through the curriculum and works with the DSL to respond to trends identified through incidents, pupil voice or monitoring.
- **All Staff:** model safe and professional technology use, maintain appropriate supervision, follow the Acceptable Use requirements, remain alert to online safety concerns and report safeguarding concerns to the DSL without delay using the school's agreed safeguarding procedures.
- **Pupils:** are expected to follow the pupil Acceptable Use requirements, use school technology responsibly, respect others online and report anything that concerns them.
- **Parents and Carers:** are encouraged to work with the school, reinforce age-appropriate online safety expectations and inform the school where an online issue outside school may affect a pupil's safety or wellbeing in school.

6. Safe use of technology and acceptable use

- Use of school networks, devices, accounts, cloud services and online platforms is subject to the school's Acceptable Use requirements. Access is provided for authorised educational and school-business purposes.
- Users must not attempt to bypass security, filtering or monitoring controls; install unauthorised software; use another person's account; share passwords; or deliberately access, create or distribute illegal, inappropriate or harmful material.
- School accounts must be protected with the security controls required by the school. Suspected compromise, phishing, malware, unauthorised access or loss of a device containing school information must be reported promptly.
- Staff must maintain professional boundaries in all digital communication with pupils and families and use school-approved communication routes. Personal social media or messaging accounts must not be used to establish inappropriate contact with pupils.

7. Mobile phones, smart technology and BYOD

The school operates a mobile-phone-free school day for pupils in line with statutory guidance from September 2026. References to mobile phones in this section include smartwatches and other communication or smart technology where the school determines that similar controls are required.

- Pupils must not have access to or use mobile phones, smartwatches or other personal communication devices during the school day. Any individual exception must be necessary, proportionate and agreed in advance by the Headteacher/DSL, for example where a specific medical, SEND or safeguarding need requires it.
- Personal devices must not be used by pupils to photograph, record or livestream other pupils or staff on school premises or during school activities unless this has been expressly authorised for an educational purpose.
- Staff, governors, volunteers and visitors must not use personal devices to photograph, film or record pupils, or to store school/pupil information, unless there is explicit school authorisation and an approved secure process.
- Personal devices must not be used to access, download or retain sensitive school information unless the school has specifically authorised the arrangement and required security controls are in place. Loss, theft or compromise of an authorised personal device used for school business must be reported immediately.
- Personal hotspots, tethering or mobile data must not be used to bypass the school's filtering, monitoring or network controls. Pupil use of personal hotspots or tethering is prohibited.
- Where a personal device is authorised under the school's BYOD arrangements to connect to the designated school network or school systems, the user remains subject to the school's Acceptable Use, data protection, cyber security and safeguarding requirements. BYOD or remote-access changes must be considered as part of the school's filtering and monitoring review.

8. Filtering and monitoring

The school uses SENSO and network/hardware filtering arrangements as part of its wider safeguarding provision. Detailed responsibilities, checks, escalation routes and review arrangements are set out in the school's Filtering & Monitoring Policy.

- Filtering and monitoring are only part of the school's safeguarding response. No system can be completely effective, so appropriate supervision, curriculum education, staff vigilance and clear reporting routes remain essential.
- The school reviews its filtering and monitoring provision at least once every academic year and also when a safeguarding risk is identified, working practices change (including BYOD or remote access), new technology or generative AI tools are introduced, major software changes occur, or network/device configuration changes materially.
- The review considers the school's pupil risk profile, what is blocked or allowed, the coverage and limitations of systems, off-site use of school-managed devices, the use of personal devices, and whether dynamic, personalised or AI-generated content can be appropriately managed.
- Monitoring alerts and reports are accessible only to authorised personnel and are handled in accordance with safeguarding and data protection requirements.

Safeguarding concerns arising from monitoring are escalated promptly to the DSL and outcomes are recorded.

9. Generative artificial intelligence (AI)

- Only AI tools that have been approved for school use may be used with pupils or for school business where approval is required by the school's technology arrangements.
- Staff and pupils must not enter confidential, safeguarding, special-category or other sensitive personal data into public or unapproved AI services. Personal data may only be used in an approved system where there is a lawful, secure and transparent basis for doing so.
- AI output must be treated as potentially inaccurate, biased or inappropriate and must be checked by a competent person. AI must not replace professional judgement in safeguarding, behaviour, assessment or other high-impact decisions.
- Pupils' use of generative AI must be age appropriate, purposeful and supervised. Teaching should address risks such as deepfakes, impersonation, manipulated images, inappropriate chatbot interactions, misinformation, bias, privacy and copyright/intellectual-property concerns.
- Introducing a new generative AI product triggers appropriate safeguarding, filtering/monitoring, cyber security, procurement and data protection consideration before use.
- All use of artificial intelligence for school purposes must also comply with the school's Artificial Intelligence Policy.

10. Managing online safety incidents

- **Immediate safeguarding concerns:** must be reported to the DSL or deputy without delay and recorded through CPOMS in accordance with the Safeguarding and Child Protection Policy. Staff must not investigate beyond what is necessary to establish the basic facts and keep a child safe.
- **Illegal or high-risk content:** must not be copied, forwarded or unnecessarily viewed. The DSL will determine the appropriate response and whether advice or referral is required from children's social care, police, CEOP or another relevant agency.
- **Nude/semi-nude or sexualised images:** must be managed in accordance with current safeguarding guidance. Staff must not view, print, copy or save an image unless specifically directed under an agreed safeguarding process.
- **AI-generated sexual imagery:** AI-generated or digitally altered sexual imagery involving children, including 'deep nudes' or sexualised deepfakes, must be treated as a safeguarding concern and reported immediately to the DSL or deputy DSL and recorded on CPOMS in accordance with safeguarding procedures.
- **Cyber security or data incidents:** such as phishing, malware, account compromise, unauthorised disclosure or device loss must also be reported promptly through the school's IT/data protection procedures. Safeguarding implications must be considered.
- **Behaviour incidents:** online behaviour that affects the school community may be addressed under the Behaviour Policy even when it occurs outside school, where the school has a legitimate basis to act. Safeguarding concerns always take priority.

Records should capture the concern, action taken, decisions made and outcome. Patterns and trends are reviewed to inform curriculum, staff training, filtering/monitoring and wider safeguarding practice.

11. Staff training and professional practice

- Online safety forms part of safeguarding induction and regular safeguarding updates for staff. Training reflects current risks, school systems, reporting routes and relevant changes in statutory guidance.
- Staff with responsibility for filtering, monitoring or access to monitoring information receive appropriate role-specific training, including the safeguarding significance of alerts and the need for lawful, proportionate and confidential handling of monitoring data.
- Staff are expected to understand the professional-boundary requirements that apply to email, messaging, social media, photographs, video, personal devices, remote working and use of AI.

12. Data protection and privacy

Personal data processed under this policy will be handled in accordance with the school's Data Protection Policy, the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and other applicable data protection legislation.

- Where filtering or monitoring systems process user activity, alerts, screenshots, search terms, messages or other personal data, access is restricted to authorised personnel and information is retained only for as long as required by the school's safeguarding, legal and records-management arrangements.
- The school will maintain appropriate privacy information explaining relevant monitoring. A Data Protection Impact Assessment (DPIA) will be completed before introducing a new filtering/monitoring system or making significant changes where required.
- Third-party online services, EdTech and AI products must be considered for privacy, security, safeguarding and contractual suitability before they are approved for use.

13. Monitoring and review

- This Online Safety Policy is reviewed at least annually and sooner where there is a significant safeguarding incident, a material change in guidance or law, or a substantial change in the school's technology or working practices.
- The DSL, Computing Coordinator/Digital Lead and IT support review incident themes and pupil/staff feedback to identify emerging risks and necessary actions.
- The annual filtering and monitoring review is recorded, includes appropriate senior leadership, DSL, IT support and governor involvement, and identifies actions and follow-up responsibility.
- Relevant changes are communicated to staff, pupils, parents/carers and governors as appropriate.

14. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR).
- The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.
- All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy

What ?	Probable Content	Why ?	Who ?	Where ?	When ?
User/account/device and online activity data	User/account details, device information and filtering/monitoring alerts where generated	Safeguarding, online safety, security and incident response	Authorised DSL/SLT/IT support and approved provider staff where necessary	Approved school systems and filtering/ monitoring services	Retained in accordance with the school's retention schedule, safeguarding requirements and provider arrangements
Online safety and safeguarding incident records	Details of concerns, individuals involved, decisions, actions and outcomes	To safeguard pupils and maintain an appropriate record of concerns and actions	DSL/deputies and other authorised safeguarding staff	CPOMS and secure safeguarding records	In accordance with safeguarding-record retention requirements
Personal data used in approved EdTech or AI services	Relevant pupil/staff information necessary for the approved service	Teaching, learning or authorised school business	Authorised staff/pupils and approved service providers as appropriate	Approved school or third-party systems	Only for as long as necessary for the approved purpose and applicable retention requirements

- As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
		✓