Online Safety Policy

St George's CE Primary School

September 2026

Date of issue	September 2026
Policy owner	Executive Headteacher / DSL
Approved by	Governing Body
Date approved	
Statutory framework	
Next review	September 2027

1. Purpose and ethos

St George's CE Primary School recognises that technology is an important part of children's education and of modern life. Our Christian vision and values underpin our approach: pupils should learn to use technology safely, responsibly, respectfully and wisely.

Online safety is a safeguarding responsibility. This policy sets out how St George's protects and educates pupils and staff in their use of technology, identifies and responds to concerns, and manages the risks associated with school systems, devices, online services and emerging technologies.

2. Scope

This policy applies to all pupils, staff, governors, volunteers, visitors and other users of school digital systems. It applies to school-owned devices and networks and, where relevant to safeguarding, behaviour or professional conduct, to the use of personal devices, social media and online services.

It should be read alongside the Child Protection and Safeguarding Policy, Positive Relationships and Behaviour Policy, Staff Code of Conduct, Data Protection Policy, PSHE including RSE Policy, Teaching and Learning Policy and relevant acceptable-use arrangements.

3. Statutory and national guidance

The policy has been written with regard to current national requirements and guidance, including:

- Keeping Children Safe in Education 2026 (KCSIE);
- DfE Teaching online safety in schools guidance;
- DfE Filtering and monitoring: core standard and Cyber security: core standard;
- DfE Generative artificial intelligence (AI) in education guidance and Generative AI product safety standards;
- DfE Data protection in schools guidance, including the 2026 updates;
- the statutory Relationships Education and Health Education requirements;
- the Prevent duty and the school's wider safeguarding responsibilities;
- UK GDPR, the Data Protection Act 2018 and relevant changes under the Data (Use and Access) Act 2025.

4. The four areas of online risk

St George's uses the four broad areas of online risk identified in KCSIE when considering safeguarding, curriculum, filtering and monitoring:

Area	Examples of risk
Content	Exposure to illegal, inappropriate or harmful material, including sexual content, violence, racism, misogyny, self-harm or suicide content, radicalisation and extremism, misinformation, disinformation, conspiracy theories and AI-generated harmful content.
Contact	Harmful interaction with other users or AI applications, including grooming, exploitation, peer pressure, harassment, adults posing as children and unsafe interactions with chatbots or simulated relationships.
Conduct	Personal online behaviour that increases harm, including bullying, sharing intimate images, harmful or abusive messages, misuse of personal information, copyright infringement and creating, sending or receiving manipulated or AI-generated intimate images.
Commerce	Risks such as scams, phishing, inappropriate advertising, in-app purchasing, financial exploitation and gambling-related content.

5. Roles and responsibilities

5.1 Governing Board

- has strategic responsibility for safeguarding, including online safety;
- ensures appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least annually;
- ensures the school has appropriate cyber-security arrangements and acceptable-use expectations;
- receives assurance from leaders that identified risks and actions are being managed.

5.2 Executive Headteacher and Head of School

- ensure this policy is implemented consistently and resourced appropriately;
- ensure staff understand their responsibilities and receive appropriate training;
- work with the DSL and IT support to ensure filtering, monitoring and cyber-security arrangements remain effective;
- ensure new technologies and services, including AI products, are considered from safeguarding, data-protection and security perspectives before use.

5.3 Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for safeguarding and online safety. The DSL considers online safety within safeguarding practice, checks relevant filtering and monitoring reports, responds to concerns and provides appropriate assurance to governors.

5.4 Staff

All staff are responsible for modelling safe and professional use of technology, supervising pupils appropriately, following acceptable-use and data-protection requirements, and reporting online-safety or safeguarding concerns promptly to the DSL.

5.5 IT support

IT support has technical responsibility for maintaining the school's filtering, monitoring and cyber-security systems, providing appropriate reports and alerts, supporting checks and reviews, and escalating technical or safeguarding concerns through agreed school procedures.

6. Filtering and monitoring

St George's will maintain appropriate filtering and monitoring arrangements across school-managed networks, services and devices. Filtering is preventative and is intended to restrict access to illegal, inappropriate and potentially harmful content. Monitoring supports the identification of concerning activity and does not replace effective staff supervision.

- Filtering and monitoring arrangements will be reviewed at least once each academic year by appropriate members of senior leadership, the DSL and IT support, with governor involvement.
- Additional review will take place when significant safeguarding risks, new technology, generative-AI tools, new devices, major software changes or changes in working practice are introduced.
- Checks will be recorded and will consider whether systems operate effectively on relevant school-managed devices and services.
- Filtering will aim to block harmful and inappropriate content without unreasonably restricting teaching and learning.
- Monitoring alerts and reports will be accessible only to appropriately authorised and trained staff.
- Safeguarding concerns arising from monitoring will be dealt with through the Child Protection and Safeguarding Policy.
- No filtering system is completely effective; staff supervision, education and professional curiosity remain essential.

7. Teaching online safety

Online safety is taught through the curriculum, including Relationships and Health Education, PSHE, computing and relevant opportunities across other subjects. Teaching will be age and stage appropriate and will respond to emerging risks.

- healthy, respectful online relationships and behaviour;
- privacy, personal information, passwords and digital footprints;
- how to recognise unreliable information, misinformation, disinformation and manipulated content;
- online bullying, harassment, grooming and exploitation;
- sharing images, consent and the permanence of online content;

- age restrictions and why they exist;
- how algorithms, advertising and persuasive design can influence users;
- how to report concerns, block users and seek help from a trusted adult;
- appropriate understanding of AI-generated material, deepfakes and the fact that digital content may be false or manipulated.

8. Pupil use of technology

Pupils may use school technology only for authorised educational purposes and under appropriate supervision. They must follow staff instructions and the school's acceptable-use expectations.

- Pupils must not attempt to bypass filtering, monitoring or security controls.
- Pupils must not access, create, store or share illegal, harmful, discriminatory, sexual or otherwise inappropriate material.
- Pupils must not use another person's account or share passwords.
- Pupils must report accidental access to inappropriate material or any online concern to a member of staff immediately.
- Pupils must treat others respectfully online and must not use technology to bully, intimidate, impersonate or harass others.
- Pupils must not take or share photographs, video or audio of others using school devices unless specifically authorised as part of a supervised school activity.

9. Mobile phones and personal devices

Children are not permitted to bring mobile phones into school. This supports safeguarding, reduces distraction and helps prevent inappropriate photography, messaging, social-media use and access to unfiltered content during the school day.

Any exceptional arrangement must be agreed in advance by the Head of School. Staff use of personal devices must comply with the Staff Code of Conduct, safeguarding requirements and data-protection expectations. Personal devices must not be used to photograph or record pupils unless specifically authorised under an agreed school procedure.

10. Artificial intelligence (AI)

10.1 School position on pupil use

Pupils at St George's CE Primary School are not permitted to use generative artificial intelligence tools or open-access AI chatbots as part of school learning. They must not use AI to generate, rewrite or complete work that is submitted to school as their own.

The school will nevertheless teach children, at an age-appropriate level, that AI exists and that AI-generated information, images, audio and video may be inaccurate, biased, unsafe or deliberately manipulated. This forms part of pupils' online-safety and digital-literacy education.

10.2 Staff use of AI

Teachers and other authorised staff may use generative AI to support their professional work, including planning, generating ideas, creating documents, producing templates and developing draft resources. AI is a support tool and does not replace professional knowledge, judgement, accountability or safeguarding responsibilities.

When using AI, staff must:

- use only services that are appropriate for professional use and comply with school expectations;
- never enter confidential, sensitive or identifiable information about a pupil, parent/carer, member of staff or family into an open or unapproved AI system;
- not upload identifiable pupil work, photographs, safeguarding records, medical information, SEND information, assessment information or other personal data to an AI service unless the school has specifically approved the system and the proposed processing is lawful;
- check AI-generated content carefully for factual accuracy, bias, suitability, safeguarding concerns and age appropriateness before using it;
- edit and adapt AI-generated material so that it is appropriate for the pupils and the intended purpose;
- respect copyright, intellectual-property and licensing requirements;
- remain professionally accountable for any planning, resource, letter, document or template they use, regardless of whether AI helped to produce it;

- never use AI as the sole basis for a safeguarding decision, assessment judgement, SEND decision, disciplinary decision or other decision that significantly affects a child.

10.3 Approval and review of AI tools

The school may restrict or block AI services that have not been approved. Before a new AI product is adopted for school use, leaders will consider safeguarding, age restrictions, data protection, privacy, security, filtering and monitoring, contractual terms and the DfE generative-AI product safety standards. A data protection impact assessment will be completed where required.

Because St George's does not permit pupil use of generative AI, access to such tools may be filtered or restricted on pupil accounts and devices. The school will review this position as technology, statutory guidance and pupils' needs develop.

11. Data protection, privacy and images

Personal data must be handled in accordance with the school's data-protection arrangements. Staff and pupils should share only the minimum information necessary for an authorised purpose. School systems, accounts and approved services must be used for school business where required.

- Images and recordings of pupils will be taken, stored and shared only for legitimate school purposes and in accordance with school procedures and privacy information.
- Personal information must not be posted on public or personal social-media accounts.
- New online platforms, monitoring systems or significant changes to existing systems will be considered for data-protection impact and a DPIA undertaken where required.
- Monitoring must be lawful, proportionate and transparent; privacy information will explain relevant monitoring arrangements.

12. Social media and online communication

Staff must maintain professional boundaries online. School communication with pupils and families must take place through approved school channels. Staff must not use personal social-media accounts to communicate privately with pupils and must follow the Staff Code of Conduct in relation to online conduct and social media.

Staff must not discuss school business on social media. This includes confidential or sensitive information relating to pupils, families, colleagues, school incidents, safeguarding matters, complaints, staffing matters or the internal business of the school. Staff must not post, comment on, share or engage with online content in a way that could breach confidentiality, compromise safeguarding, undermine professional relationships or bring the school into disrepute. School business must be communicated through the school's approved professional channels. ClassDojo is the school's main parent communication platform and must be used professionally and in accordance with safeguarding and data-protection expectations.

13. Cyber security

St George's will work towards and maintain the DfE cyber-security standards appropriate to schools. Cyber security is both a technical and safeguarding responsibility.

- accounts will be individual wherever practicable and access will be limited according to role;
- users must protect passwords and use multi-factor authentication where required;
- school devices and software will be appropriately licensed, maintained and updated;
- anti-malware, firewall, backup and recovery arrangements will be maintained;
- staff must be alert to phishing, suspicious links, social engineering and fraudulent requests;
- cyber risks will be assessed and reviewed, and significant incidents will be reported and managed through the appropriate school, data-protection and national reporting routes;
- staff must report suspected compromise, loss of a device, suspicious activity or a personal-data breach immediately.

14. Responding to online-safety incidents

Where an online incident may constitute a safeguarding concern, staff must report it to the DSL without delay and follow the Child Protection and Safeguarding Policy. Evidence should be preserved appropriately without staff unnecessarily viewing, copying or forwarding harmful material.

The school will distinguish, where appropriate, between a safeguarding response, a behaviour response, a cyber-security response and a data-protection response. More than one response may be required. Where illegal activity is suspected, the school will seek appropriate advice and make referrals or reports where necessary.

15. Online bullying and child-on-child abuse

Online bullying, sexual harassment, abuse, coercion or harmful sharing between children will be taken seriously whether it occurs on school systems or outside school where it affects a child's safety, welfare or school life. Concerns will be managed in accordance with the Child Protection and Safeguarding Policy and Positive Relationships and Behaviour Policy.

Staff will not dismiss online abuse as banter or an inevitable part of growing up. Victims will be supported, risks considered and action taken in a child-centred and proportionate way.

16. Remote and home learning

Where pupils access school-provided online learning away from the school site, the same expectations of respectful behaviour and safe use apply. Staff will use approved systems and maintain professional boundaries. Families will be given appropriate information about safe access and supervision where necessary.

The school's prohibition on pupils using generative AI to produce schoolwork applies equally to work completed at home and submitted to school.

17. Staff training and awareness

Online safety is included within safeguarding training and updates. Staff will be made aware of filtering and monitoring responsibilities, emerging online risks, cyber security, data protection and safe use of AI. Staff with specific responsibility for monitoring systems will receive appropriate training for that role.

18. Working with parents and carers

St George's will support parents and carers to understand online risks and the school's expectations. Information may be shared through ClassDojo, newsletters, workshops or other school communication. Parents and carers are encouraged to talk regularly with children about their online activity, age restrictions, privacy and how to seek help.

19. Monitoring and review

The Executive Headteacher, Head of School and DSL will monitor implementation of this policy. Filtering and monitoring provision will be reviewed at least annually and whenever significant technological or safeguarding changes make an additional review necessary. The Governing Board will review this policy annually, or sooner following significant changes to statutory guidance, technology or school practice.

20. Key references

- Department for Education: Keeping Children Safe in Education 2026.
- Department for Education: Teaching online safety in schools.
- Department for Education: Meeting digital and technology standards in schools and colleges – Filtering and monitoring: core standard.
- Department for Education: Meeting digital and technology standards in schools and colleges – Cyber security: core standard.
- Department for Education: Generative artificial intelligence (AI) in education.
- Department for Education: Generative AI: product safety standards.
- Department for Education: Data protection in schools.
- Department for Education: Using AI in education settings – support materials.