St George's Central CE Primary School and Nursery

Online Safety Policy

Policy updated by Miss Beswick (Computing lead): March 2026

Policy approved by Governors: April 2026

Chair of Governors

Headteacher

Policy shared with staff and shared on the school website: April 2026

'Never settle for less than your best'

Jesus said, 'I am the light of the world. Whoever follows Me will not walk in darkness, but will have the light of life.' John 8:12

ONLINE SAFETY POLICY

Our school motto

Never settle for less than your best.

Our Vision

Following in the footsteps of Jesus, each member of our community will flourish as resilient, respectful and adaptable individuals prepared for life's journey. Along the way we will encourage and inspire each other to continue growing as beacons of light in our own lives and the wider world.

Our Mission Statement

St. George's Central seeks to provide quality education rooted in the Christian faith, serving the spiritual, moral, and educational needs of the community of which it is part.

Introduction

This policy applies to all members of the school community (including staff, students/pupils, Governors, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school. It aims to safeguard and protect all members of St. Georges Central Primary School and Nursery community online.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Computing/Online Safety Lead:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Receives reports of online safety incidents and monitors incidents to inform future online safety.
- Reports regularly to Senior Leadership Team.

Technical staff:

Computing Technician and Computing Co-ordinator is responsible for ensuring:

- That the school's computing infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the online safety technical requirements outlined in any relevant Local Authority online safety policies and guidance.
- That users may only access the school's networks through a properly enforced password protection policy.

Teaching and Support Staff are responsible for ensuring that:

• They have an up to date awareness of online safety matters and of the current school online safety policy and practices.

• They have read, understood and signed the school Acceptable Use Agreement Form for Staff, Volunteer and Community Users.

• They report any suspected misuse or problem to the Online Safety Co-ordinator /Headteacher/ Computing Co-ordinator for investigation/action/sanction.

Designated Safeguarding Leads will be trained in online safety issues and be aware of the potential for serious Child Protection issues to arise from:

• Sharing of personal data.

• Access to illegal/inappropriate materials.

• Inappropriate on-line contact with adults/strangers.

• Potential or actual incidents of grooming.

• Cyber-bullying Students/pupils.

• Are responsible for using the school computing systems and mobile technologies in accordance with the Acceptable Use Agreement Form for children (EYFS and KS1) (KS2).

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platforms such as SeeSaw, YouTube and information about national/local online safety campaigns/literature.

Parents and carers will be responsible for:

• endorsing (by signature) the Student/Pupil Acceptable Use Policy (This also applies when accessing a school laptop for home learning).

• accessing the school computing systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school computing systems or Learning Platform as part of the Extended School provision will be expected to sign the Acceptable Use Agreement Form for Staff, Volunteer and Community Users before being provided with access to school systems and technology.

Social Media

Personal Accounts – Staff are not permitted to access personal social media accounts through any school equipment unless authorised to do so by the headteacher. The school Facebook account can be accessed through school equipment. All school X accounts must ensure children under the age of 13 are not following their account. This essentially means that only parents/carers from school should be following the X account. School X accounts must follow the online safety lined out in this document.

Online Safety and Training

Education – pupils

Online education will be provided in the following ways:

- Online safety will be provided as part of Computing/PHSE and will be regularly revisited – this will cover both the use of Computing and new technologies in and outside school. Children will be given access to different scenarios to analyse with adults and peers.
- Children will be taught across all curriculum areas to develop critical awareness of the online content they encounter. They will be guided in assessing the accuracy, reliability, and validity of information, including material generated through artificial intelligence platforms

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff will receive online safety training/updates as part of good practice, ensuring that they fully understand the school online safety expectations and Acceptable Use Policies.
- Updates from Computing Lead/Designated Safeguarding Lead and PSHE where appropriate.

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods. Where it is indicated that the method or device is allowed at certain times, these are clearly outlined below:

	Staff & other adults				Students/Pupils			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to school (stored in allocated lockers)								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on other camera devices								
Use of personal hand held devices eg PDAs, PSPs								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of chat rooms / facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								
Use of school X accounts								
Use of school equipment to access personal banking					N/A	N/A	N/A	N/A

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Mobile phones may be brought to school	Phones must be stored in allocated lockers. The Designated Safeguarding Leads in school will give discretion to certain staff members.	If children are walking home on their own – all mobile phones must be handed to a designated member of staff at the extensions external doors. Phones will be securely stored in class baskets until the end of the day.
Taking photos on other camera devices	During school visits/trips/events	Use for curriculum activities on school devices under supervision of staff.
Use of personal email addresses in school, or on school network	Any e mails on personal e mail accounts must be sent to an approved school e mail address.	Not permitted in school
Use of chat rooms / facilities	For educational purposes only eg online safety lessons	Use for curriculum activities under supervision of staff.
Use of instant messaging	For educational purposes only eg online safety lessons	Use for curriculum activities under supervision of staff.
Use of social networking sites (X)	'X' can be used to share information about school but only adults can follow school 'X' accounts.	Can be used by children with permission of an adult
	Personal 'X' accounts cannot be accessed using school equipment	No personal accounts to be accessed through school equipment
Use of social networking sites (Facebook)	School Facebook account can be accessed through school equipment	Cannot be accessed by children
	Personal Facebook accounts cannot be accessed through school equipment.	No personal accounts to be accessed through school equipment
Use of blogs	For educational purposes only eg online safety lessons	Can be used by children with permission of an adult

Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are increasingly accessible to staff, pupils, and parents/carers, including platforms such as ChatGPT and Copilot. While AI can enhance teaching and learning, it also presents potential risks, including its misuse to cause harm.

We recognise that AI may be used to create misleading or harmful content, such as 'deepfakes'—fabricated images, audio, or video that appear genuine. This includes the creation of inappropriate or abusive material using an individual's likeness. Any use of AI to intimidate, harass, or bully pupils will be addressed in accordance with the school's anti-bullying and behaviour policies.

Staff must remain vigilant regarding the risks associated with emerging AI technologies. When introducing or using new AI tools within the school environment, staff are expected to complete an appropriate risk assessment to ensure safe and responsible use.

Cyber Bullying

What does cyber bullying mean?

Cyberbullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.

As more and more people are using mobile phones and the internet, people may use these to bully. As a result of this, St George's Central actively discourages children bringing mobile phones to school. If it is absolutely essential that a child needs to bring in a mobile phone, it must be switched off as soon as the child is on the school site, it will be handed to a member of staff as soon as the child arrives at school, it will then be securely held in classrooms and is only switched on when the childl leaves our school site. This is done to remove the risk of cyber bullying at school using mobile phones.

At St. George's Central CE Primary and Nursery, we understand that cyber bullying can happen at any time and can happen in places that you consider to be safe or personal. Sending a rude or hurtful text message, for example, means that cyber bullying could take place anywhere and at anytime of the night or day and the person receiving this may be at their home.

Sometimes cyber bullying may happen because someone did not think about or did not understand the consequences. Online actions are generally different to actions or things said face to face with a person. Because of this, we must think about the following things:

- The distance between the bully and the person being bullied means we do not know the situation that has caused this. The message may have been intended as a joke but not understood and seen as hurtful and nasty. The person sending the message cannot see that their message has upset someone and so they can't sort out the misunderstanding.
- Sending a single message or image that may be embarrassing or upsetting, to the sender may be seen as a one-off, but because of technology this message or image could be sent on to others or posted online for other people to see.

Digital equipment, computers, mobile phones and the internet are now common parts of a child's environment and learning. Many children rely on technology to keep in touch with people and to learn, communicate and socialise with groups. Technology can play a positive, productive and creative part in the activities and social development of young people. Staff and parents/carers must be aware of the technologies being used, and how these are being used by children, they may be used in the wrong way. If staff and parents/carers understand children's online activities, it can help them to respond to situations in the right way. Adults need to talk to children about what they do with technology and what they are worried about so that being safe online can be discussed.

Types of Cyber bullying:

- Threats sent by mobile phone, email, via comments on websites, social networking sites or message boards.
- Repeated, unwanted texting or texting over a long period that is not wanted.
- Posting upsetting or cruel remarks about someone online, or name-calling using a mobile device.
- Online exclusion by refusing to return or acknowledge messages, deleting from friendship lists or using 'ignore' functions deliberately to cause harm and upset.

- Identity theft, unauthorised access & pretending to be someone else.
- Publicly posting, sending or forwarding personal or private information or images.
- Any abuse using technology.
- Using AI tools to generate, alter or impersonate individuals to create harmful, embarrassing or degrading content.
- Using AI chatbots to generate hurtful or malicious responses

Anti-Cyber bullying Code:

Children will be taught the seven key messages in the anti-cyber bullying code as follows:

1) Always respect others.
2) Think before you send.
3) Don't let anyone, other than parents/carers, know your passwords.
4) Block the bully – responsible websites & services allow blocking and reporting someone who is behaving badly.
5) Don't retaliate or reply.
6) Save the evidence – this will help to show others what is happening so that action can be taken.
7) Make sure you tell!

The above points are also taught through online safety education through SMART rules.

The use of digital photographs and videos

The use of digital/video images plays an important part in learning activities. Students/pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website, YouTube and occasionally in the public media. The school will comply with the Data Protection Act /GDPR and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names. Parents are requested to sign the permission form (Appendix 5 in Acceptable Use Policy) in to allow the school to take and use images of their child, and for their child to access the internet. This ensures compliance with GDPR guidelines.

Monitoring and review

This policy will be reviewed on an annual basis with the next scheduled review date being April 2027.