E-Safety Policy

"Our soul waits for the Lord; he is our help and our shield."
Psalm 33:20

Ensuring we are fully protected against fraud, viruses, or online harassment and ensuring young people learn to safeguard themselves through curriculum, we protect the way we navigate a tumultuous online world.

Saint Cecilia's Church of England School is committed to providing great educational opportunities for all our pupils and students. The safety and welfare of our pupils and students is of the utmost importance. We hope to ensure that pupils and students can safely access new technology and learn how to participate in the digital world without compromising their safety and security.

This policy sets out how we will keep pupils/students at Saint Cecilia's e-safe, whether using technology within the school's provision or at home.

This policy has been written in reference to:

- Keeping Children Safe in Education (2023)
- NSPCC
- South West London Grid for Learning

Linked policies include:

- Behaviour Policy
- Child Protection Policy
- Anti-bullying Policy
- Preventing Extremism and Radicalisation
- Use of Photography and Video Policy

This policy applies to all members of the Saint Cecilia's school community including staff, pupils, students, volunteers, parents and carers, and visitors.

Rationale for the E-Safety Policy

The impact of technology on the lives of all citizens increases yearly, particularly for children and young people who are keen to explore new and developing technologies. Technology is transforming the way that schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. Developing technology brings opportunities; it also brings risks and dangers including:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, and sharing of personal information
- Online grooming
- Radicalisation and extremism

- The sharing and distribution of personal images without consent
- The sharing and distribution of indecent images
- Inappropriate communication and contact with others
- Cyber-bullying
- Sexting
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive use which may impact on social and emotional development and learning
- Physical, sexual, emotional, financial and psychological abuse online and through social media platforms

These risks are real and as our pupils, students and staff use technology more, we need to ensure they understand the risks, minimise the risks, know the consequences of risky behaviour and be explicitly taught to use technology safely and responsibly.

Furthermore, the school also has a responsibility to model safe and responsible internet use concerning content, images and videos that are posted by the school including all website content, use of Microsoft Teams, virtual events and exhibitions.

Roles and responsibilities

The Headteacher and Governing Body will ensure the e-Safety Policy is regularly monitored and reviewed, updated and carried out responsibly by all stakeholders. The Leadership Team will examine new and emerging technologies for educational benefit before use in school is allowed with clear guidelines.

All staff will familiarise themselves with the policy and adhere to the recording, monitoring and reporting of any incidences of risky behaviour by pupils or students. In face to face or virtual teaching and learning settings, staff will model and monitor safe and responsible use of technology as per the school's virtual learning guidance. Staff will also receive training to clarify expectations, applicable roles, and responsibilities in relation to filtering and monitoring when using the school's Wi-Fi and school software.

Parents and carers have a responsibility to support the school's e-Safety policy and ethos behind safety procedures and the behaviour policy. They should also seek help from the school and other appropriate agencies if they or their child encounters risks or concerns online. They should also take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Parents and carers are also invited to attend parent events which will include addressing concerns regarding social media and phone use. Parent event leaders will also be able to give support and information on how to keep devices safe as well as approaching e-safety conversations at home. Information and support can also be found on the school website.

The school ICT systems capacity and security will be reviewed regularly by the Business Manager. The school will work in partnership with the LA, DfE and the Internet Service Provider to ensure systems to protect staff, students and pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it will be reported to the ICT Network Office.

Effective E-Safety

Curriculum

E-safety is taught, mainly through PSHE and ICT lessons by trained or specialist teachers. In addition, e-Safety may also be discussed formally in assemblies, during mentor meetings, in the Library, the Bethany Centre or the PSMs office.

PSHE and Computing explicitly teach:

- Appropriate and available Internet and ICT use in school including guidance on mobile phone use, personal devices, printing, Internet use and e-mails;
- Internet and social media addiction including symptoms, causes, impacts and healthy internet use;
- Identity and the impact of social media on identity, mental health and well-being including selfies, online profiles, sharing and using information;
- Fake news, hoaxes, how to spot it, how to respond to it;
- Recognising, responding to and reporting online grooming;
- Risky behaviour including taking and sharing images that are deemed indecent images, peer pressure, self-esteem, confidence and respect;
- Cyberbullying, spamming, trolling including why this is done, the impact and how to manage, deal and cope as a victim or bully;
- Pornography access online including impact on young people and healthy relationships;
- Clickbait, phishing, card fraud, gambling and being able to differentiate between legitimate and fake emails and phone calls, and how to respond appropriately;
- Recognising and responding to risky or negative material and images regarding mental health;
- Effective and responsible use of new technologies in research, including the skills of knowledge location, retrieval and evaluation.

Monitoring and Reporting

Pupils and students can report incidences of concern, unsafe, risky or bullying behaviour as a result of or through new technologies using the Behaviour Policy and the school's iwanttotalk@saintcecilias.london e-mail address.

Staff can report to line managers, members of the Leadership Team or the Safeguarding Team through CPOMS.

All reports will be investigated and outcomes will be based on guidance of the Behaviour Policy.

ICT

The school's network manager ensures safe and secure broadband including the effective management of filtering unsafe or risky content. Each member of staff, pupil and student has a

protected log in and password to access appropriate and relevant school systems and the Internet. Any unsafe use of this will be reported immediately and managed through the school's Behaviour Policy.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

GDPR

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Should any future communication with parents be by e-mail, there will be protection of that data. All data will be removed from redundant hard drives before their disposal.

E-mails

Pupils may only use approved e-mail accounts on the school system. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mails sent to an external organisation should be written carefully and where appropriate authorised before sending, in the same way as a letter written on school headed paper. If issues are sensitive, staff should always seek advice through line management prior to sending e-mail.

Review

The governing body will review this policy annually, delegating overall responsibility for its monitoring to the head teacher, through the CTL for PSHE.

Action	Committee	Date
Review and Approve	Curriculum & Standards Committee	January 2024
Next Review	Curriculum & Standards Committee	January 2026

Saint Cecilia's Church of England School
Sutherland Grove, London SW18 5JR
info@saintcecilias.london
020 8780 1244
www.saintcecilias.london