St Paul's
C of E Primary School

A place to belong

E-safety Policy

Chair of Governors Approval:	**Tom Mitchell**
Headteacher Approval:	**Christie Clarke**
Member of Staff Responsible:	**Hannah Severn**
Reviewing Committee:	**FGB**
Date to be reviewed:	**Jan 2026**
Statutory / Non Statutory:	**Statutory**

St Paul's C of E Primary School

A Place to Belong

Our Christian Vision

Our school is a family where everyone feels safe, happy and valued, and is supported to achieve their full potential.

We will develop compassionate and caring individuals who depend on one another, are highly motivated, and have a life-long love of learning in preparation for the future.

Our Core Values

All that we do is underpinned by the core Christian values of *Family (Koinonia), Compassion, Perseverance and Forgiveness*

"Though we are many, we form one body, all joined together as members of the whole. We each have different gifts, according to the grace given to each of us. We must use them wisely."
Romans 12:5-8

E-safety Policy

Aims of the Policy

Our lives are surrounded by technology. At St Paul's Primary School we embrace technology as we believe it enriches children's learning experiences. As a school we engage with a variety of different online resources, using a range of hardware. This policy is designed to ensure that children and staff can use these technologies effectively and safely, outlining a number of ways in which we can best manage the technologies available at school.

E-Safety at St Paul's CE Primary School

At St Paul's Primary School, we understand that computer technology is an essential resource for supporting teaching and learning to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks. Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not covered by the school network protection and it is, therefore, imperative that pupils are educated on the risks involved with using the internet. Children are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an E-safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENCO, DSL and DDSLs, classroom teachers, support staff, young people and parents, LA personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. E-safety is a child protection issue, and indeed it should be an extension of general safeguarding and led by all staff, so that, for instance, cyber bullying is considered alongside real-world bullying.

An E-safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure regular monitoring and reviews of policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective E-safety program.

Above all, E-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.
The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Roles and Responsibilities

It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils. Our school use a web filtering system provided by CYC in partnership with Vital. This filtering system is specifically designed for Education.

The school provides pupils with an e-mail system. This is restricted to internal communications only (both incoming and outgoing). The E-safety officer, Christie Waite, is responsible for ensuring the day-to-day E-safety in the school, and managing any issues that may arise. The headteacher is responsible for providing all staff training relating to E-safety.

All staff ensure they understand and adhere to our Acceptable Use Agreement, which has been shared with all staff.

All pupils ensure they follow our school E-safety rules which are shared in class regularly. Pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

The headteacher is responsible for communicating with parents regularly and updating them on current E-safety issues and control measures.

376383104. **Teaching and Learning**

Why the internet and digital communications are important

376384840.376384392. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

376384840.376384393. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

376384840.376384394. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

376384840.376384395. Staff model safe and responsible behaviour in their use of technology during lessons.

376384840.376384396. Teachers remind pupils about their responsibilities when using the internet and use the E-safety rules with their classes, see the appendices.

Internet use will enhance learning

376384840.376384397. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

376384840.376384398. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

376384840.376384399. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

376384840.376384400. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

376384840.376384401. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

376384840.376384402. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

376384840.376384403. Pupils will be taught how to report unpleasant internet content to their class teacher. This can be done anonymously, or in person. Teachers will remind pupils about their responsibilities when using the internet and use the E-safety rules with their classes, see appendices. Class teachers will then inform the E-safety lead, who is the headteacher of any E-safety issues raised.

376384840.376384404. The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files – without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know and report any abuse, including online bullying, and how to seek help if they experience any problems using the internet and related technologies.

376384840.376384405. When planning computing, teachers plan internet use carefully that is age appropriate and supports the learning objective linked to the curriculum. Staff use appropriate websites and child friendly search engines when accessing the web with pupils.

376384840.376384406. The school will remind pupils about their responsibilities through our E-safety school rules.

376384840.376384407. All staff will model safe and responsible behaviour in their own use of technology during lessons.

376384841. **Managing Internet Access**

Information System Security

376384841.376384392. School ICT systems security will be reviewed regularly.

376384841.376384393. Virus protection will be updated regularly. Our Virus protection is provided by Vital.

376384841.376384394. Security strategies will be discussed with the LA. City of York Council provide our network security.

Email

376384841.376384395. Pupils may only use approved email accounts on the school system.

376384841.376384396. Pupils should not receive any emails from other accounts as all accounts are filtered by Vital however if an email is received children must immediately tell a teacher.

376384841.376384397. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

376384841.376384398. The forwarding of chain letters is not permitted.

Published Content and the School Website

376384841.376384399. Staff or pupil personal contact information will not be published.

376384841.376384400. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

376384841.376384401. Uploading of information is restricted to our website authorisers.

376384841.376384402. The school website complies with statutory DfE guidelines for publications.

376384841.376384403. The point of contact on the website is the school address and telephone number. The school uses a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual email identities will not be published.

376384841.376384404. Photographs published on the web do not have names attached.

376384841.376384405. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Social Networking and Personal Publishing

376384841.376384406. The school will control access to social networking sites and consider how to educate pupils in their safe use.

376384841.376384407. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

376384841.376384408. Pupils and parents will be advised that the use of social network spaces outside of school should be monitored by the parent. Workshops for parents by the local police are offered by the school.

Managing Filtering

376384841.376384409. If staff or pupils come across unsuitable online materials, the site must be reported to the headteacher.

376384841.376384410. Senior staff including governors, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

376384841.376384411. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

376384841.376384412. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

376384841.376384413. Staff and visitors must adhere to the Acceptable Use policy.

376384841.376384414. Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by any other means is forbidden.

376384841.376384415. Pupils who bring a mobile phone to school will leave their mobile phones with their class teacher during the school day.

Protecting Personal Data

376384841.376384416. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

376384842. **Policy Decisions**

Authorising Internet Access

376384842.376384392. All staff will read and sign the Acceptable Use Policy on induction.

376384842.376384393. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

376384842.376384394. At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

376384842.376384395. At EYFS, KS1 and KS2 children will use the agreed rules regarding E-Safety, see appendices.

376384842.376384396. Any person not directly employed by the school will be asked to read the Acceptable Use Policy before being allowed to access the internet from the school site.

Assessing Risks

376384842.376384397. The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.

376384842.376384398. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access. The school will take action if any inappropriate material is found by a member of staff or pupil.

376384842.376384399. The school should audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.

Handling E-safety Complaints

376384842.376384400. Complaints of internet misuse will be dealt with by the headteacher.

376384842.376384401. Any complaint about staff misuse must be referred to the headteacher.

376384842.376384402. Complaints of a child protection nature must be dealt with in accordance with school child protection policy.

376384842.376384403. Pupils and parents are informed of the complaints policy.

376384842.376384404. Parents will be informed of the consequences for pupils misusing the internet.

376384842.376384405. Discussions will be held with the headteacher to establish procedures for handling potentially illegal issues.

Community use of the Internet

376384842.376384406. The school will liaise with local organisations to establish a common approach to E-safety.

376384842.376384407. St Paul's have worked with both the NSPCC and the Local Police force to teach children and parents about E-safety.

Cyber Bullying and Abuse

376384842.376384408. Cyber bullying can be defined as “Any form of bullying which takes place online or through smartphones and tablets.” - BullyingUK

376384842.376384409. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with School child protection policy.

376384842.376384410. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

376384842.376384411. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are discussed and taught through computing and PSHE.

376384842.376384412. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying policy. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.

376384842.376384413. There are clear procedures in place to support anyone in the school community affected by cyber bullying.

376384842.376384414. All incidents of cyber bullying reported to the school will be recorded on CPOMS.

Sexual Exploitation/Sexting

376384842.376384415. Sexting between pupils will be managed through our anti-bullying procedures.

376384842.376384416. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

376384842.376384417. The headteacher will support anyone in the school community affected by sexting.

376384842.376384418. All incidents of sexting reported to the school will be recorded.

Radicalisation or Extremism

376384842.376384419. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism. Staff adhere to the school Extremism and Anti Radicalisation policy.

376384842.376384420. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent

extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.

376384842.376384421. Staff understanding that radicalisation could be through the internet or social media and staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

376384842.376384422. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

376384843. **Communications Policy**

Introducing the E-safety Policy to Pupils

376384843.376384392. E-safety rules and guidance will be discussed with classes with pupils regularly, see appendices.

376384843.376384393. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

376384843.376384394. A programme of training for staff around e-safety will be developed by the headteacher.

376384843.376384395. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

Staff and the E-safety Policy

376384843.376384396. All staff will be given the school E-safety Policy and have its importance explained.

376384843.376384397. All staff will adhere to the Acceptable Use Policy.

376384843.376384398. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

376384843.376384399. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

376384843.376384400. Staff will always plan appropriate computing lessons to ensure children are safe online.

Enlisting Parents' Support

- Parents' attention will be drawn to the school E-safety Policy in an e-safety leaflet, newsletters, the school brochure and on the school website.
- The school will maintain a list of e-safety resources for parents.
- The school will have a page on its website dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

376381984. **Monitoring and Review**

376381984.376382992. The E-safety Policy will be evaluated on an annual basis, taking into account the school's E-safety calendar, the latest developments in ICT and the feedback from staff/pupils.

376381984.376382993. This policy will also be reviewed by the governing body; any changes made to this policy will be communicated to all members of staff.

376381984.376382994. Members of staff are required to familiarise themselves with this policy as part of their induction.

Useful Resources for Teachers and Parents

Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
NSPCC - Share Aware	https://www.nspcc.org.uk/keeping-children-safe/online-safety/
National Online Safety	https://nationalonlinesafety.com/

Appendix 1

EYFS/KS1 E-safety rules

St Paul's
C of E Primary School

A place to belong

St Paul's C of E Primary School
Our E-safety Rules

Follow these simple rules to keep safe and be fair to others.

- I will be careful with the computers/chromebooks/iPads.
- I will only use technology for school tasks and homework.
- I will not send messages to anyone, unless my teacher says it is OK.
- I will never give out my name, home address, telephone number, or any other information about myself or my family.
- I will tell my teacher if I find any words or pictures which make me feel unhappy or confused.

Appendix 2

KS2 E-safety rules

St Paul's
C of E Primary School

A place to belong

St Paul's C of E Primary School
Our E-safety Rules

At school, we think that computers are a fantastic aid to learning. That is why we have an up a range of technology and opportunities to develop computing skills through interesting programmes in school.

The internet opens up wonderful possibilities for finding out about anything that interests us. It is up to all of us to make sure we use it wisely.

Follow these simple rules to keep safe and be fair to others:

I will take good care of all the computing equipment and treat it with respect.

I will use the computers/chromebooks/iPads only for school tasks and homework.

I will not send or receive E-mails to or from anyone, unless I have the teacher's permission.

Any messages I do send will always be polite and responsible.

I will not open or login to other children's accounts or folders.

I will never give out my surname, home address, telephone number, or any other information about myself or my family

I will let a teacher know if I find any pictures or writing which make me feel uncomfortable. I know I will not be in trouble for this

I understand that the school will, from time to time, check the computer files and monitor internet sites I have visited