

St. Paul's C of E Primary School

Documentation Information and Control

On-Line Safety (Internet Use) Policy

Current Status: Revised December 2019, 2021, and 2023

Review date: December 2025

Persons responsible for review: The Governing Body in consultation with the Head Teacher

Reference to other documents: Child Protection Policy and Safeguarding Policy
Computing Policy
Keeping Children Safe in Education: Statutory guidance for schools and colleges, DfE September 2023

On-line Safety (Internet Use) Policy

1. Rationale

- 1.1 St Paul's School was established in 1862 to serve Almighty God and the community by providing, within a biblical Christian ethos, a broad, balanced, and engaging education and learning experience.
- 1.2 St Paul's School is an inclusive school in which, through the provision of a broad, balanced, and engaging curriculum and within a caring and supportive environment, each pupil is motivated to develop and flourish as he or she acquires skills for life and a love of learning.
- 1.3 The Governing Body recognises that all people owe their existence to God and are dependent upon him for their preservation day by day.
- 1.4 The Governing Body acknowledges that mankind, male and female, was created in and as the image of God and thus, from conception to the grave, all people are always to be shown care, love and respect.
- 1.5 The Governing Body acknowledges that all people are accountable to God for all that they think, say, and do, including the way they treat others.
- 1.6 The Governing Body recognises, without prejudice to a parent's or a carer's responsibility for their child(ren), that those who work in St Paul's School act in the place of parents and carers.
- 1.7 The Governing Body recognises that the Internet is a huge resource which is increasingly used as a means of gathering and publishing information on a worldwide scale and that it offers exciting opportunities for both communication and the dissemination of information.

- 1.8 The Governing Body also recognises that, because some information accessible on the Internet is inappropriate, harmful or offensive (see clause 3.5 below), every precaution must and shall be taken to prevent access and exposure to unacceptable material.
- 1.9 The Governing Body shall ensure that, in line with the 2023 edition of Keeping Children Safe in Education, the school has robust filtering and monitoring procedures and software in place to protect pupils and staff in school settings safe from on-line harmful and ill-legal material (see *paragraph 1.13 below*).
- 1.10 On-line safety shall be reflected as required in all relevant policies.
- 1.11 On-line safety shall be considered as a running and interrelated theme when devising and implementing policies and procedures and when planning curriculum, staff training, the role and responsibilities of the Designated Safeguarding Lead (DSL), and parental engagement.
- 1.12 On-line safety addresses the following categories of risk:
- (1) *Content*:
exposure to illegal, inappropriate or harmful content, e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
 - (2) *Contact*:
subjected to harmful on-line interaction with other users, e.g. peer on peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
 - (3) *Conduct*:
personal on-line behaviour that increases the likelihood of, or causes, harm, e.g. making, sending and receiving explicit images, the consensual and non-consensual sharing of nudes and semi-nudes and / or pornography, sharing other explicit images, and on-line bullying.

- (4) *Commerce:*
risks such as on-line gambling, inappropriate advertising, phishing and or financial scams.

1.13 **Appropriate Filtering and Monitoring**

- (1) A service level agreement with the Local Authority ensures that appropriate filtering and monitoring systems are in place.
- (2) If a pupil or staff member discovers unsuitable sites or material, they shall report the concern immediately to the DSL and report the URL of the site to IT services.
- (3) All users will be informed that use of our systems are monitored, and that monitoring is in line with data protection, human rights, and privacy legislation.
- (4) Any access to material believed to be illegal will be reported immediately to the appropriate agencies.

1.14 **Educating Pupils about on-line safety**

- (1) In **Key Stage 1** pupils will be taught to:
 - use technology safely and respectfully, keeping personal information private; and
 - identify where to go for help and support when they have concerns about content or contact on the internet or other on-line technologies.
- (2) In **Key Stage 2** pupils will be taught to:
 - use technology safely, respectfully and responsibly;
 - recognise acceptable and unacceptable behaviour; and
 - identify a range of ways to report concerns, content and contact.
- (3) By **the end of Key Stage 2** pupils will know:
 - that people sometimes behave differently on-line, including by pretending to be someone they are not;
 - that the same principles apply to on-line relationships as face to face relationships including the importance of respect for others on-line including when anonymous;

- the rules and principles for keeping safe on-line, how to recognise risks, harmful content and contact and how to report them;
- to critically consider on-line friendships and sources of information including awareness of the risk associated with people they have never met;
- how information and data is shared and used on-line;
- how to respond safely and appropriately to adults they may encounter on-line.

2. Procedures for the use of the Internet by pupils

- 2.1 The school shall provide Internet use consent forms for the use of parents/carers.
- 2.2 Parents/carers shall be required to give consent for:
 - (1) their child(ren) to use the Internet, and,
 - (2) for photographs of and work by their child(ren) to be published on the school web site.
- 2.3 Acceptable Use Agreements will be signed by all staff, governors, visitors, and volunteers (*see appendices 1-13*).
- 2.4 The school shall not be held responsible for the nature and content of materials accessed through the Internet nor held liable for any damages arising from the use of Internet facilities.
- 2.5 A responsible adult shall always supervise pupils using the Internet.
- 2.6 Access to all computer / iPad facilities within school shall be for educational purposes only.
- 2.7 Pupils shall acknowledge the source of all material used in presented work.
- 2.8 When communicating with others via the Internet appropriate and acceptable language shall always be used.

- 2.9 Any pupil receiving inappropriate messages shall report the incident immediately to their supervisor and the Head Teacher.
- 2.10 As there is no way of checking the integrity of external computer users, no user in school shall reveal any personal detail to other Internet users.
- 2.11 All communications shall be sent only from a name(s) and address(es) sanctioned by a teacher.

3. Procedures for the use of the Internet by staff using loaned laptop computers

- 3.1 All Internet activity in school shall be restricted to that which is lawful and shall be for educational purposes and professional development only.
- 3.2 Access to the Internet from the school shall only be by means of the authorised account and an appropriate private password.
- 3.3 Access to the Internet from home and terminals away from the school shall be made through reliable Internet Service Providers.
- 3.4 Individual teachers shall be responsible for their own Internet and e-mail activity and shall take appropriate measures to ensure that there is no inappropriate use by third party users.
- 3.5 All incidents of accidental contact with inappropriate material shall be logged. Inappropriate material is material of a pornographic, racist and offensive nature as defined in the Computer Misuse Act 1990, the Obscene Publications Acts of 1959 and 1964, the Protection of Children Act 1978, the Children Acts of 1989 and 2004, and the Sexual Offences Act 2003.
- 3.6 All e-mails shall meet the same professional levels of language and content as letters or other media and none shall be sent anonymously.
- 3.7 Staff shall not communicate with pupils through social networking sites and should be mindful of their professional status when placing personal information on social networking sites.

- 3.8 All software downloaded on to loaned laptops / iPads shall support teaching and learning and, when appropriate, shall be properly licensed. The terms of the school's Data Protection registration shall be adhered to and applied.
- 3.9 Laptops / iPads and other network devices shall be regularly connected to the school's network system (preferably once a week during term time) to benefit from the automatic updating of security and antivirus software.
- 3.10 Breaches of the conditions outlined in this policy could lead to disciplinary action and the withdrawal of Internet access and loan privileges. Serious misuse could lead to dismissal on the ground of serious misconduct and criminal prosecution.

4. Use of cameras and mobile phones

- 4.1 At St Paul's School all possible steps are taken to ensure that an environment exists in which children, parents and staff are kept safe from the inappropriate recording, storage and use of images.
- 4.2 In paragraphs 4.3 - 4.8 below a clear framework is provided to ensure that:
- (1) the use of cameras and the storage of images reflect good practice,
 - (2) the safeguarding needs of the pupils are met, and
 - (3) staff are not distracted from their work with children.
- 4.3 The term 'camera' includes mobile phones, iPads and other equipment with the capacity to record and store images.
- 4.4 Mobile phones and personal cameras must not be used by any member of staff, volunteer or helper, either inside or outdoors, during contact with children. The only exception is the teacher in charge during a visit out of school whose mobile phone is the emergency contact number for school.
- 4.5 Mobile phones may be used to make or receive personal calls during break times providing children are not present.

- 4.6 All images taken by members of staff or volunteers at school or on visits out of school may only be taken on school cameras.
- 4.7 All such images shall remain the property of the school.
- 4.8 All images taken on school cameras must be uploaded to the school computer system at the earliest opportunity and deleted from the camera.
- 4.9 Images must not be published in any way without the knowledge of the Head Teacher and permission from the parents or carers of children in the pictures.

5. Review

The Governing Body shall review this policy every other year.

KS1 Acceptable Use Agreement

Name of
learner:

Class:

- I will always ask a teacher or suitable adult if I want to use the computer, tablets or cameras
- I will only open activities that an adult has told or allowed me to use
- I know that I must tell an adult if I see something on a screen that upsets me, or of which I am unsure.
- I will keep my passwords safe and I will never use someone else's password
- I know personal information such as my address and birthday is never to be shared on-line
- I know I must never communicate with strangers on-line
- I will always be polite when I send e-mails on work on OneNote.
- I know that my parent/carer will be told if I do not follow this agreement.

Signed:

KS2 Acceptable Use Agreement

Name of learner:

Class:

- I will only access computing equipment when a trusted adult has given me permission and is present
- I will not deliberately look for, save or send anything that could make other people upset.
- I will immediately inform an adult if I see something that worries me, or that I know is inappropriate
- I will keep my username and password secure; this includes not sharing it with others
- I understand what personal information is and I will never share my own or other's personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Mirodo or SATS Companion.
- In order to help keep me and others safe, I know that the school checks my files and on-line sites that I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as emails and OneNote carefully. I will tell an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions will be taken.
- Before I share, post or reply to anything on-line, I will T.H.I.N.K

T

Is it True?

H

Is it Helpful?

I

Is it Inspiring?

N

Is it Necessary?

K

Is it Kind?

Signed:

Acceptable use of the school's ICT systems and internet:

Agreement for staff, governors, volunteers and visitors.

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- use them in any way which could harm the school's reputation
- access social networking sites or chat rooms
- use any improper language when communicating on-line, including in emails or other messaging services
- install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- share my password with others or log in to the school's network using someone else's details
- take photographs of pupils without checking with teachers first
- share confidential information about the school, its pupils or staff, or other members of the community
- access, modify or share data I'm not authorised to access, modify or share, or
- promote private businesses, unless that business is directly related to the school.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (*staff member/governor/volunteer/visitor*):

Date: