



St Paul's School  
FOUNDED 1509

## E-Safety Policy

Author/reviewer responsible:	Director of Digital Learning and Innovation	Date of last review:	06/25
Reviewed by:	E-Safety Committee	Date of authorisation:	08/25
Authorised by resolution of:	Safeguarding Committee	Date of next review:	06/26

**This policy is available on the Handbook page of the School Intranet and policies page of the School website and can be made available in large print or other accessible format if required; such requests can be made by email to [policyquery@stpaulsschool.org.uk](mailto:policyquery@stpaulsschool.org.uk)**

## 1. Introduction

- 1.1 It is the duty of St Paul's School (**SPS**) and St Paul's Juniors (**SPJ**) to ensure that every pupil in its care is safe; the same principles apply to the digital world as apply to the real world.
- 1.2 New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people.
- 1.3 SPS and SPJ understand the responsibility to educate pupils about how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse, radicalisation and identity theft, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.
- 1.4 The breadth of issues classified within online safety is considerable and ever evolving, but can be generally categorised into four areas of risk, often known as the '4 Cs':
  - **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
  - **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography).
  - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If there is concern for any pupil or staff then this concern can be reported to the Anti-Phishing Working Group (<https://apwg.org/>).

## 2. Scope and Review

- 2.1 Both this policy and the Acceptable Use Policies apply to all members of the St Paul's Community (including staff (including contract staff), pupils, Governors, parents, visitors) who have access to and are users of the School's IT systems, both in and out of the School. It covers both fixed and mobile phones internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.) and all devices owned by pupils and staff brought onto school premises (laptops, tablets, mobile phones, etc). This policy also applies to behaviour taking place outside of school, where it is linked to membership of the School.
- 2.2 This policy, supported by the Acceptable Use Policies (AUPs), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies and procedures:

- Acceptable Use / IT Policies (including SPJ iPad and BYOD guidance);
- Anti-Bullying Policy;
- Behaviour Management Policy;
- Data Protection Procedure;
- Health and Safety Policy;
- Mobile Phone Policy;
- Privacy Notice;
- PSHE Policies (SPJ & SPS);
- Remote Learning & Safe Working Guidance;
- Safeguarding and Child Protection Policy;
- Social Media Policy;
- Use of Artificial Intelligence Policy
- SPJ Academic Integrity Policy
- Use of Digital Images and Recording Policy
- Staff Code of Conduct.

### **3. Roles and responsibilities**

#### **Governors**

3.1 The Governing Body of the School is responsible for periodically reviewing the effectiveness of the e-safety policy.

3.2 There is a designated Governor responsible for safeguarding who oversees the work done on online safety, amongst other elements of safeguarding with the Deputy Head (Pastoral) and Designated Safeguarding Lead (DSL).

#### **Designated Safeguarding Lead (DSL)**

3.3 The DSL has lead responsibility for online safety, including overseeing and acting on filtering and monitoring reports and checking the filtering and monitoring systems.

3.4 The DSL will:

- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

### **e-Safety Officers**

3.5 There are three e-Safety Officers at the school. The Lead e-Safety Officer is the Director of Digital Learning and Innovation and they are supported by the Director of Computing at SPJ and the IT Manager.

3.6 The Lead e-Safety Officer will:

- Chair the e-Safety Committee;

3.7 The e-Safety Officers will

- promote an awareness of and commitment to online safety education/awareness raising across the school;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- liaise with curriculum leaders to ensure the online safety curriculum is planned, mapped, embedded and evaluated;
- receive regular updated training to allow them to understand how digital technologies are used and are developed (particularly by pupils) with regards to the areas defined in KCSiE: content, contact, conduct and commerce.
- Provide regular communication with parents and carers to keep them informed of e-safety matters and how children can stay safe online.

3.7 The e-Safety Officers (Director of Digital Learning and Innovation, Director of Computing at SPJ and the IT Manager), Senior Management Team and the e-Safety Committee have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by organisations such as CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Partnership.

3.8 They are also responsible for ensuring that teaching and support staff are adequately trained about online safety (including responsibilities in relation to filtering and monitoring) and they are aware of the School's procedures that should be followed in the event of a data breach of suspected breach of online safety. **e-Safety Committee**

3.9 The e-Safety Committee has the following members: Director of Digital Learning & Innovation , DSL (Whole School), DSL (SPJ), IT Manager, e-Safety Officer (SPJ); Head of PSHE (SPS); Head of PSHE (SPJ); Director of Operations.

3.10 The role of the committee is to:

- Produce/review/monitor the relevant e-Safety policies;
- conduct an annual e-Safety internal audit
- ensure the filtering policy is applied and updated on a regular basis;

- monitoring systems are implemented and regular updated

### **IT Support Department**

3.11 The IT Support Department has a key role in maintaining safe infrastructure at the School and keeping abreast of technical developments. They are responsible for the security of the School's hardware and its data. They monitor the use of the internet and emails, maintain content filters and support the work of the DSL in managing breaches.

### **Teaching and Support Staff**

3.12 As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

3.13 New staff receive information on SPS and SPJ's e-Safety and ICT Acceptable Use and Social Media policies and training on how online safety interacts with child safeguarding as part of their induction.

3.14 All staff receive regular information and training (at least annually) on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the relevant guidance and legislation e.g. KCSiE and UK GDPR regulations. All supply staff [and contractors] also receive our e-Safety Policy on arrival at school.

3.15 All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policies which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

3.16 Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. 3.6.6 an incident relating to e-safety occurs then the school's appropriate e-Safety Officer and DSL/DDSL must be informed immediately.

### **Pupils**

3.17 Pupils are responsible for using the School's IT systems in accordance with the ICT Acceptable Use Policy, and for letting staff know if they see those systems being misused.

3.18 Pupils should avoid plagiarism (as outlined in the SPJ Academic Integrity Policy) and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

## Parents

- 3.19 It is essential for parents to be involved in the promotion of online safety, both in and outside of School. The School provides up to date information to parents via the Parental Portal, Weekly Newsletters, online webinars and in person events.

## 4 e-Safety in the curriculum and school community

- 4.1 IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.
- 4.2 The school provides opportunities to teach about e-safety within a range of curriculum areas and Computer Science lessons. Educating pupils on the dangers of technologies that may be encountered both inside and outside school will also be carried out via PSHE, as well as informally when opportunities arise.
- 4.3 The school recognises that technology, and risks and harms related to it, evolve, and change rapidly. As such, our approach to online safety is regularly reviewed by the e-Safety officers and as a minimum this occurs on an annual basis.
- 4.4 An e-Safety curriculum is provided as part of Computer Science, PSHE and other lessons and is regularly revisited
- 4.5 Key e-Safety messages are reinforced as part of a planned programme of assemblies. Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- 4.6 Pupils are helped to understand the need for the Pupil AUP agreement and encouraged to adopt safe and responsible use both within and outside school. Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging.
- 4.7 At age-appropriate levels, pupils are also taught about relevant laws applicable to using the internet, such as data-protection and intellectual property. All pupils are taught about respecting other people's information and images. They are educated about the risks associated with taking, use, sharing, publication and distribution of images (including nudes and semi-nudes).
- 4.8 Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- 4.9 Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the schools' Anti-bullying Policies). Pupils should approach the Designated Safeguarding Lead, the Deputy Designated Safeguarding Leads or the e-Safety

Officers as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

- 4.10 The School recognises that not all Parents feel equipped to protect their son when they use electronic equipment at home. Therefore, the School arranges discussions, both online and in person, with advice about online safety and the practical steps parents can take to minimise the potential dangers to their son, without curbing their natural enthusiasm and curiosity.

## **5 Use of the internet, social media and email**

- 5.1 Expectations and guidance on appropriate use of the internet, social media and email by staff and pupils are outlined in the Code of Conduct, ICT Acceptable Use and Social Media policies.
- 5.2 Staff and pupils must immediately report to the e-Safety Officers the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- 5.3 There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work, staff and pupils should contact the Director of Digital Learning and Innovation, Director of ICT (SPS) or Director of Computing (SPJ) for assistance.

## **6 Password security**

- 6.1 Pupils and staff have individual school network logins, email addresses and storage folders on the server.
- 6.2 Staff and pupils are required to use multi-factor authentication when accessing the school systems offsite and encouraged to use biometric security when available.
- 6.3 All pupils and members of staff should:
- use a strong password (usually containing ten characters or more, and containing upper- and lower-case letters as well as numbers);
  - not write passwords down; and
  - should not share passwords with other pupils or staff.

## **7 Filtering and Monitoring**

- 7.1 Staff, pupils and visitors should be aware that all internet usage via the school's systems and its wifi network is monitored and the filtering and monitoring systems apply to all users and any device connected to the School's network.
- 7.3 The DSL has tasked the IT Manager with reporting any attempted breaches of the filtering systems. The DSL and High Master will be informed of any staff flagged by the system and an

investigation will then take place. Pupils which are flagged by the system are reported to the DSL, e-Safety Officers and the pupil's Undermaster (for SPS) or Head of Year (for SPJ). An investigation, carried out by e-Safety officer and Undermaster/Head of Year will then commence.

- 7.4 The DSL has tasked the IT Manager with ensuring that the School's filtering systems are up to date and are monitoring appropriate sites/words. The IT Manager completes an audit of the system, at least annually, to ensure it is fit for purpose and market leading. The report generated from this audit is delivered to the E-Safety Committee and the Safeguarding Governors Committee.

## **8 Use of school and personal devices**

### **Staff**

- 8.1 School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use their allocated school device for school work. When they are not using a device staff must ensure that it is locked or in a locked environment to prevent unauthorised access.
- 8.2 Staff at SPS and SPJ are permitted to bring in personal devices for their own use.
- 8.3 Personal telephone numbers and email addresses may not be shared with pupils or parents / carers and staff may not contact a pupil or parent / carer using a personal telephone number or email address, unless it has been authorised by the Designated Safeguarding Lead.

### **Pupils**

- 8.4 SPJ pupils use iPads on a 1:1 basis and are expected to use them in line with the Pupil Acceptable Use Policy.
- 8.5 SPS pupils have access to their own devices in line with the Mobile Phone policy and the Pupil Acceptable Use Policy.
- 8.6 The school recognises that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 4G and 5G). This access means some children whilst at school could harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually and view and share pornography and other harmful content.
- 8.7 Whilst the School's firewall will pick up and block many instances of online harm using wi-fi, it is the School's recommendation that parents/guardians install filtering and monitoring software on pupil devices. Further advice and guidance can be found at:  
<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>  
<https://saferinternet.org.uk/online-issue/parental-controls>

## **9 Artificial Intelligence (“AI”)**

- 9.1 The School only permits the use of generative AI tools on the School’s devices/systems in specific circumstances as referred to in the Acceptable Use Policies for staff and pupils and Artificial Intelligence Policy.

## **10 Data protection**

- 10.1 The school takes its compliance with data protection law seriously. Please refer to the Data Protection Policies, Privacy Notices, and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.
- 10.2 Staff and pupils are expected to save all data relating to their work to their password protected device or to a school-approved drive unless with specific written consent from one of the e-Safety officers .
- 10.3 Staff may only take sensitive information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks and auto-forwarding of emails to personal or non-school email addresses is prohibited.
- 10.4 Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school’s IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the Director of Digital Learning and Innovation, Director of Computing (SPJ) or IT Manager.
- 10.5 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to one of the e-Safety Officers.

## **11 Safe use of digital and video images**

- 11.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.
- 11.2 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should

recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

## **12 Complaints**

12.1 As with all issues of safety at SPS and SPJ, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Officers in the first instance, who will undertake an immediate investigation. Please see the [Complaints Policy](#) for further information.

13.2 Incidents of, or concerns around, e-safety will be recorded on the pupil's file and reported to the school's Designated Safeguarding Lead, in accordance with the school's Safeguarding and Child Protection Policy.