St Paul's School
FOUNDED 1509

E-Safety Policy

Author/reviewer responsible:	DSL	ISI DOC CODE:	7
Reviewed by:	ICT Committee	Date of last review:	07/23
Authorised by resolution of:	Safeguarding Committee	Date of authorisation:	08/23
Applicable:	SPS & SPJ	Date of next review:	07/24

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

Introduction

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; and the same principles apply to the digital world as apply to the real world. 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. Our pupils are therefore taught 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.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Applications;
- Online communities via games consoles;
- Virtual and augmented reality technology; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Policies (AUPs) and the roles and responsibilities documents (for all staff, visitors and pupils), 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;
- Anti-Bullying Policy;
- Behaviour Management Policy;
- Bring Your Own Device Procedure;
- 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 Procedures;
- Staff Code of Conduct.

Whilst exciting and beneficial both in and out of the context of education, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies.

At SPS and SPJ, we understand the responsibility to educate our pupils on e-safety issues; 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.

Both this policy and the Acceptable Use Policies (for all staff, visitors and pupils) cover both fixed and mobile phones and internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.). It also covers all devices owned by pupils and staff brought onto school premises (laptops, tablets, mobile phones, etc).

Roles and responsibilities

The e-Safety Officers (the Director of ICT at SPS, the Director of Computing at SPJ and the IT Manager), Senior Management Team and the ICT Committee have responsibility for ensuring this policy is upheld by all members of the school community. The roles and responsibilities of all stakeholders is outlined in the E-Safety Roles & Responsibilities document. 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. 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.

Filtering and Monitoring

It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. As part of this process the school has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness. The school fully complies with the Department for Education's published filtering and monitoring standards which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs

Roles and responsibilities for filtering and monitoring at the School:

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

- 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 Safegaurding Governors Committee.

Staff awareness

New staff receive information on SPS and SPJ's e-Safety and Acceptable Use policies and training on how online safety interacts with child safeguarding as part of their induction. 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 safeguarding of children within the context of e-safety. All supply staff [and contractors] also receive our e-Safety Policy on arrival at school.

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.

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.

If an incident relating to e-safety occurs then the school's appropriate e-Safety Officer and DSL/DDSL must be informed immediately.

E-Safety in the curriculum and school community

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.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT 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.

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, and extremism.
- **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/).

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.

An e-Safety curriculum is provided as part of ICT, PSHE and other lessons and is regularly revisited 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.

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. Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

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 school's Anti-bullying Policy). 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.

Use of school and personal devices

Staff

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.

Staff at SPS and SPJ are permitted to bring in personal devices for their own use.

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

SPJ pupils use iPads on a 1:1 basis and are expected to use them in line with the Acceptable Use Policy. SPS pupils have access to their own devices in line with the Mobile Phone policy and the Bring your own device Procedure.

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. The School's firewall will pick up and block many instances of online harm however 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

Use of internet and email

Staff

The school encourages and supports staff in their use of digital technologies, sites and appliances in the course of their work (administrative, teaching, co-curricular, pastoral) with pupils but requires that any such use is informed and fully consistent with our standards and policies. All staff must read and make sure they understand the Codes of Conduct before engaging in any such activity:

- everyone should seek the permission of the e-Safety Officer before creating accounts or posting material on social sites or apps where the material is related to the school.
- on social sites and apps, closed groups should be used where possible.
- 'friending' between staff and pupils on social media is never appropriate.
- there should be no communications between staff and pupils on personal social media. Electronic communications between staff and pupils should be conducted on school systems, such as school email, or the school virtual learning environment. Exceptions to this can only be made via application to the DSL and E-Safety Officers.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored.

Staff should be aware that all internet usage via the school's systems and its wifi network is monitored.

Staff 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.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the school into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links or material which is discriminatory or offensive.

It is advised that staff should not add parents as friends or follow them on social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school e-mail addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Pupils should be aware that email communications are monitored.

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, pupils should contact the Director of ICT (SPS) or Director of Computing (SPJ) for assistance.

Pupils should immediately report, to the e-Safety Officers or another member of staff 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.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the e-Safety Officers or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work, pupils should contact the Director of ICT (SPS) or Director of Computing (SPJ) for assistance.

Data protection

The school takes its compliance with data protection law seriously. Please refer to the Data Protection Policy, Privacy Notice, 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.

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 the e-Safety officer or IT Manager.

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.

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 ICT (SPS) or Director of Computing (SPJ) in accordance with the Data Protection Policy and Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of ICT (SPS) or Director of Computing (SPJ).

Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Where available, staff and pupils are encouraged to use biometric security and two-factor authentication. Staff and pupils are regularly reminded of the need for password security.

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.

Safe use of digital and video images

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.

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.

Complaints

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 and liaise with the Senior Management Team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Incidents of, or concerns around, e-safety will be recorded using a pastoral module form and reported to the school's e-Safety Officers and the Designated Safeguarding Lead, in accordance with the school's Safeguarding and Child Protection Policy.