Online safety policy

Action	Policy to be reviewed annually		
	Owner	**Date**	**Completed**
Review	Assistant Head, Teaching, Learning & Innovation	April 2023	✓
Approve	Education Committee	9 May 2023	✓

To be published on the following:	
Staff Portal	✓
Student Portal	✓
Parent Portal	✓

Online safety policy

To whom this policy applies

This policy applies to staff and students, also providing guidelines and expectations for parents.

What this policy is for

This policy aims to promote responsible and effective use of digital and online communication (including the use of the internet, social media, digital technology, and mobile phones & devices).

Legal framework

- Keeping Children Safe in Education

Other relevant school policies

The school recognises that digital and online safety is an extension of the school's wider commitment to safeguarding, therefore this policy draws together the principles and practices set out in a number of other policies and processes, and should be read in conjunction with the resources below:

- Safeguarding (child protection) Policy
- Child on Child Abuse Policy (previously peer-on-peer abuse)
- Data Protection Policy
- Behaviour Policy (including rewards and sanctions)
- Anti-bullying Policy
- Student Acceptable Use Policy
- Staff Acceptable Use Policy
- Student Device Guidelines
- Mobile phone policy
- Staff Code of Conduct
- Taking, Storing and Using Images of Students Policy
- Mental Health & Wellbeing Policy
- Online Resource Approval Procedures here
- School PSHE/RSE programme

Appendices

Content of policy

1. Aims and objectives

1.1 St Paul's Girls' School is committed to safeguarding and promoting the welfare of children and young people, and this extends to students' use of technology and their online interactions.

1.2 We recognise that technology and the internet are valuable learning tools and have become an integral part of how young people communicate, socialise, and learn. These technologies have enormous benefits: stimulating discussion, promoting creativity, enabling connectivity, and enhancing learning, but we recognise that emerging technologies also bring risks and potential dangers.

1.3 We aim to:

- Provide an online and digital environment that reduces exposure to harmful content, where students feel safe and where they have the knowledge and confidence to use technology in a safe and responsible way.
- Strike the right balance in facilitating best practice in online learning and digital workflow, while restricting opportunities for online abuse and negative behaviours resulting from unwelcome online activity.
- Promote digital and online literacy and confidence with a progressive programme of training, instruction and rules.
- Promote responsible and effective use of digital and online communication (including the use of the internet, social media, digital technology, and mobile phones & devices).
- Educate students and staff about the risks, responsibilities and potential criminal implications involved in the use of technology.
- Raise awareness of, and to counteract, instances of cyberbullying, including bullying via online chat and social media.

2. Risk

2.1 The breadth of issues classified within online safety is considerable, but can be categorised into the following areas of risk:

- Content: harm that can arise from exposure to inappropriate, distasteful, extremist, radicalising or illegal content.
- Contact: harm that can arise from interactions with other individuals online.
- Conduct: harm that can arise from how young people behave online.

2.2 In practical terms, the main online risks have been identified as:

- Privacy (data misuse; identify theft; oversharing).
- Grooming and inappropriate contact with strangers.
- Cyberbullying.
- Access to sexual, pornographic, violent, self-harm, suicidally ideated, terrorism and hate-related content.
- Fraud and allowing or seeking unauthorised access to personal information or private data.
- Infringement of copyright, plagiarism and unlawful downloading of content.
- An inability to evaluate the quality, accuracy, and relevance of information, particularly with regard to concerns about 'fake news', and the ability to be drawn into echo chambers.
- The potential for excessive or addictive use which may impact social and emotional development and/or learning.

3. Policy statements

3.1 School procedures

3.1.1 The school ensures that there are clear procedures for the restriction of unwanted online activity and processes to follow in the event of safety-related issues arising from online activity. Our processes are designed to encourage responsible and safe online activity, dovetailed with our digital education and training programmes.

We will:

- Provide a progressive system of filters, monitoring, and device management that can be adjusted for each year group and/or activity, subject to regular review, to limit students' exposure to online danger and risks while on the school's network in an age-appropriate manner and in line with a programme for preparing our students for responsible, safe and secure online activity.
- Ensure the school network is configured to support school systems on-premises as well as for remote access to school systems.
- Ensure that school acceptable use policies (AUPs) provide clear, safe and secure processes and expectations for responsible access to the school network from onsite, for remote working and when using school devices including 1:1 devices (staff and students) or BYOD devices where appropriate.
- Provide parents with students on 1:1 devices with a means to exercise parental consent for third-party resources where appropriate.
- Provide processes for staff, students and parents to report issues or concerns, and that any concern is dealt with appropriately in accordance with the Safeguarding (child protection) policy.
- Support the investigation of potential incidents of peer-on-peer abuse, including bullying, harassment or threatening behaviour in accordance with the Behaviour, Anti-bullying, and Peer on Peer Abuse policies.
- Support the investigation of incidents that may breach our student or staff AUPs, behaviour and safeguarding (child protection) policies.
- Provide staff, students and parents with clarity relating to the use of third-party online resources, including of a list of resources approved for use by the school community with conditions for their use where appropriate.

3.2 Education & Training

3.2.1 The school aims to equip students, staff and parents with an understanding of how to use technology in a safe, responsible and appropriate way and, through training, induction and the curriculum, to take measures to:

- Provide students with the knowledge and skill to:
    - develop online safety awareness.
    - behave responsibly.
    - know how to protect their personal data when online.
    - communicate appropriately when online.
    - know how to report a concern relating to online activity.
    - self-regulate their online usage.
    - develop the safe, responsible and appropriate use of technology at all times whether in school or at home.
    - have confidence in their use of technology, appropriate to their age.
    - leave the school with a good understanding of responsible online behaviour.
- Provide advice and guidance to parents on how to support their child's safe, responsible and appropriate use of technology.
- Train students and staff with core skills to support school-wide digital competence for safe online activity.
- Train key staff with specialist skills to support our training programme and reinforce/promote good practice.
- To engage with external agencies and networks to stay abreast of sector-wide best practice.
- Ensure that new staff receive safeguarding and cyber security training as part of their induction.

3.3 Technology

3.3.1 The school implements IT systems that support a safe and secure environment in which to learn and takes measures to:

- Ensure that the school's technical systems are implemented and managed according to information safety and security best practice and that their implementation is continually monitored and reviewed.

- Implement appropriate technical controls to reduce the risk of exposure to potentially harmful content, including inappropriate websites, spam and computer malware (viruses).
- Ensure that personal data is managed and protected in line with statutory requirements (The Data Protection Act 2018 and the UK General Data Protection Regulation 2021).
- Ensure that staff, students and parents are informed and, where appropriate, trained in the school's approach to technology to a standard necessary for safe online practice.
- Provide support for the school device policy.

4. Roles and responsibilities

4.1 All staff, governors and volunteers have a duty to protect children from abuse and to report matters of concern to the Designated Safeguarding Lead, see section 11 of the Safeguarding (child protection) policy. The following relates specifically to online safety:

4.2 Director of Pastoral Care

- Acts as Designated Safeguarding Lead with responsibility for child protection and the safety (including online safety) of students.
- Reviews and updates policies, procedures and documentation relating to safeguarding and child protection.
- Oversees the PSHE/RSE curriculum.
- Liaises with the Director of HR and the Director of Strategic Development to arrange a staff development programme on online safety.
- Provides students and parents with opportunities to report online trends and concerns through the portal pages.
- Works with the Online Approvals team to ensure that they are trained to triage and escalate safeguarding concerns for third-party online resource approvals and apply appropriate conditions of use for approved resources.
- Working with the Director of IT to ensure that the school filtering, monitoring, and device management settings are appropriate to protect staff and to support progressive, safe online activity for students across all age groups.
- Working with the Director of IT and the Online Approvals Team to support parents in exercising parental consent for students on 1:1 devices through the school mobile device management system.
- Working with local police and the "Safer Schools" project to deliver regular briefings to students.
- To oversee the visiting speaker policy and procedures and ensure that they apply to online activity.
- Reviews and escalates information and alerts from the school's network filtering and monitoring systems.

4.3 Director of Studies

- Oversees the curriculum and, working with the Assistant Head – Teaching, Learning & Innovation, ensures that good digital practice in the school's academic provision supports safe online activity aligned with the school PSHE programme.
- Line management of the Computer Science & Creative Technologies (CS&CT) curriculum and a programme for the development of digital skills.

4.4 Director of Strategic Development

- Oversight of the Digital Strategy Group.
- Working with the Director of IT, oversight of the school IT provision.
- Responsible for the (this) Online Safety Policy working with the Director of IT and Director of Pastoral Care.
- Working with the Director of Studies, the Assistant Head – Teaching & Learning (Innovation) and the Director of IT, has oversight and technical provision for the school's remote learning platform.
- Reviews and updates the school's AUPs and Information Security documentation in conjunction with the Digital Strategy Group

4.5 The Bursar

- Supported by the Data Protection Consultant, works with the Online Approvals Team to ensure that they are trained to triage and escalate data protection, privacy, legal and regulatory concerns for third-party online resource approvals and apply appropriate conditions of use for approved resources.

4.6 Deputy Head Co-Curriculum and Deputy Head Partnerships

- Oversight of online safety for online conferences, events and collaboration. See below.

4.7 Assistant Head Teaching & Learning (Innovation)

- Sits on the Digital Strategy Group to advise and disseminate best practice to support the online safety of our students.
- Acts as school Online Safety Officer (pastoral) working closely with the school Online Safety Coordinator (IT network).
- Organises parents' discussion evenings on the topic of digital and online safety.
- Works with the Director of Studies, Heads of Departments and the Heads of CS&CT and PSHE to ensure that digital training and workflows are progressively and consistently applied:
    - Supporting safe, secure and responsible online behaviour.
    - Preparing our students for confidence in their approach to online safety.
    - Understanding responsibility both to themselves as well as each other.

4.8 Director of IT

- Acts as the school Online Safety Coordinator (IT network) working closely with the Online Safety Officer (pastoral).
- Oversees the safety and security of the school's technical infrastructure.
- Oversees the school's network filtering and monitoring systems.
- Investigates any misuse of IT systems and equipment that may breach the Student Acceptable Use Policy or the Staff Acceptable Use Policy.
- Provides online safety advice and training to staff.
- Works with the Online Approvals Team to ensure that they are trained to triage and escalate technical concerns for third-party online resource approvals and their conditions for use.

4.9 Human Resources Department

- With Heads of Departments and staff delivering CPD, coordinates staff induction, onboarding and offboarding.
- Identifies training needs for new staff on appointment to meet school core standards.
- Works with the Strategic Development coordinator and line managers to develop training schedules for core and specialist skills.
- Ensures that new staff complete relevant training, in conjunction with their line manager and/or the Assistant Head – Teaching & Learning (Staff Development), through the pre-induction process (including online training), as specified by the Director of IT.

4.10 Director of Communications

- Responsible for public-facing online presence.
- Working with the school Data Protection Consultant to ensure that the school's public-facing resources support safe online practice and meet safe and compliant standards.
- Supports the teaching staff with content capture, images, video and audio recording and school consent & release forms for school activities.

4.11 Data Protection Consultant

- Works with the Online Approvals Team to ensure that they are trained to triage and escalate data protection, privacy, legal and regulatory concerns for third-party online resource approvals and apply appropriate conditions of use for approved resources.
- Provides first-line support for the library staff to coordinate the online approvals process.
- Works with the Director of Communications and Digital Strategy Group to ensure that the school's public-facing online presence, including websites and social media presence, meets data protection, privacy, legal and regulatory standards and that they support safe online practice.

4.12 Head of Computer Science & Creative Technologies

- Develops and delivers the CS&CT curriculum.
- Ensures that the digital skills delivered in the CS&CT foundation course support safe, secure, and responsible online behaviour.
- Educates students in the online safety and data protection aspects of digital content creation, and modelling through the consent & release forms.

4.13 Heads of Year

- Monitor and report any pastoral concerns arising out of their conversations with students, staff or parents.
- Coordinate pastoral and disciplinary response as and when needed in the case of an online safety concern.
- Supported by the Director of Pastoral Care and Online Safety Officer, working with form tutors to support them in responsibilities (below).

4.14 Head of Personal, Social, and Health Education (PSHE)

- Develops and oversees the delivery of the PSHE/Relationships and Sex Education (RSE) curriculum.
- To work with the Director of Pastoral Care, the Assistant Head – Teaching, Learning & Innovation and the Director of IT to ensure that a continuous, progressive programme of online safety training is included in the PSHE programme and, where appropriate, dovetailed with the curriculum.

4.15 Tutors

- Deliver the PSHE/RSE curriculum.
- Monitor and report any pastoral concerns arising out of their conversations with students, staff, or parents.
- To explain and reinforce school AUPs.

4.16 eLearning Team

- Deliver training and support for teaching staff and students to develop digital competence in support of safe online practice.
- To disseminate good online practice, agreed with the Digital Strategy Group, through core skills training and digital resources encouraging efficient digital workflow.
- To identify staff needs and advise the Digital Strategy Group with recommendations for meeting these.

4.17 All staff

- To read, understand and follow this Online Safety Policy.
- To adhere to the school's AUPs.
- To reinforce student acceptable use of school IT resources, promote responsible online behaviour, and escalate issues of concern.
- To follow the school's Online Resource Approval process and abide by any conditions of use for approved resources.

4.18 All students

- To adhere to the student AUP.
- To engage with the school programme of education and training for online safety.

5. Parental/guardian responsibility for students

5.1 Technical barriers can never entirely protect a student from harmful online content. Parents should be aware that whilst the school network and IT facilities are configured to support a safe and secure environment in which to learn, the same protection is not in place when using other networks, including those at home and personal data plans.

5.2 Students' mobile phone contracts are not (and cannot be) the responsibility of the school. Smartphones are likely to have an internet connection (sometimes referred to as a data, 3G, 4G or 5G

connection, for example) which may not have any content filtering in place and could, therefore, be used for unconstrained access to the internet.

5.3 Parents/guardians are expected to ensure that internet access and social media usage through personal devices and mobile contracts is appropriate to the student's age and should also be responsible for giving guidelines to students about the amount of time spent using their devices.

5.4 Whilst the school takes the actions described to ensure that the school community understands the importance of safe behaviour online, the school cannot be held responsible for inappropriate online behaviour that bypasses the school network. In light of this, **parents/guardians must also be responsible for ensuring that students are responsible for using technology in a safe and secure way and behave responsibly when online.** The full range of school disciplinary procedures will be considered in the event of any breach of this policy or the school's Behaviour Policy.

5.5 Both the school and parents have a responsibility to ensure that students have the knowledge and confidence to know what to do if they encounter content or receive communications that make them feel uncomfortable, worried or upset and are able to share their concerns in an open and supportive environment. Please see further paragraph 6 below relating to education and training.

6. Education & training

6.1 Delivery

6.1.1 St Paul's Girls' School delivers its online safety training through a combination of in-person instruction and online resources. Training may be delivered through the PSHE programme or through assemblies and presentations and form tutors. External specialists involved in internet and online safety are engaged to provide training as appropriate.

6.1.2 Online safety training should be integrated, aligned, and considered part of the whole school safeguarding approach and wider staff training and curriculum planning. It is a component of new staff induction. All students are taught about safeguarding, including online safety.

6.2 Students

6.2.1 Our approach to online safety is broad, relevant, and tailored to the concerns and risks of particular age groups. It is delivered through a combination of the school curriculum, the PSHE curriculum, assemblies, and outside speakers, which, together with the Student Acceptable Use Policy, aims to develop safe and responsible behaviour both within and outside the school. It will include the guidance for students referred to in paragraph 7.1 below.

6.2.2 Online resources that are directly linked to for schoolwork are subject to the online approval process, but students may exercise broader access to the internet as they progress through the school, following paths and accessing material that may not be directly recommended by the school. Student training and instruction are in place to ensure that students understand what is, and is not, appropriate and that they should avoid inappropriate resources or content, reporting any specific concerns that may have resulted in compromised safety and/or security.

6.3 Staff

6.3.1 The Staff Code of Conduct and the Staff AUP provide guidelines on how staff should behave and interact with students.

6.3.2 All new staff receive a safeguarding induction which includes information on online safety and guidelines on how staff should behave when online.

6.3.3 Working with the Director of Pastoral Care and Online Safety Officer, Heads of Year should communicate with their tutors about online safety issues regularly.

6.4 Parents

6.4.1 Parents play an essential role in the education of their children and in the monitoring and regulation of their child's online behaviour and are asked to be aware of the following, in particular:

- Parents/guardians are asked to support and reinforce the school approach to online safety, which is clearly stated in this policy and the school's AUPs, which can be found on the parent portal.
- The provision of parental control of student laptops for students on 1:1 school devices, outlined on the parent portal, provides the ability for parents to lift restrictions, providing parental consent within school-defined parameters when student devices are not on the school Wi-Fi system, for example at home.

6.4.2 Online safety information and awareness is provided to parents via the parent portal and the school's AUP as well as school events such as parents' discussion evenings. The Director of Pastoral Care delivers a talk to all MIV parents at the start of the academic year on the theme of online safety and risk prevention, supported by the Head of Lower School and Director of Strategic Development.

6.4.3 The school publishes its processes for online resource approval of third-party resources to support parental awareness and to promote transparency of our filtering and safeguarding systems.

6.5 Onsite and Remote Learning

6.5.1Remote Learning. The provision of remote learning is preserved for exceptional circumstances. During periods of remote and hybrid learning, in addition to the above, particular attention is drawn to the school's AUPs and school online interactive learning guidelines.

6.5.2 Online conferencing, events, and collaboration. Online conferencing is now a commonplace method for schools to collaborate and run events. Attending/hosting online events is the virtual equivalent of running/hosting a school trip. Details of the school's approach to this can be found in Appendix 2.

6.5.3 Personal data plans. The school is not responsible for personal data plans for mobile phones, laptops, tablets, internet-connected watches, and indeed any other devices that connect to the internet. A condition for permitting student personal devices in school is that students only access the intranet and the internet through the school Wi-Fi network so that they are subject to its safety and security settings. **The use of personal data plans while in school is forbidden** and parents are asked to support the school in enforcing this with their children.

6.6 Email

6.6.1 Students are inducted into the appropriate use of email and there is clear guidance in the AUPs about what is, and is not, acceptable in terms of email communication. Any inappropriate email must be reported to the student's form tutor or Head of Year immediately.

6.6.2 Transparency, openness and appropriate purpose must underpin all academic and pastoral interaction between staff and students via electronic, online and digital means.

7. Online Activity

7.1 Guidance for Students

7.1.1 Students are encouraged to seek advice if they are concerned, uncomfortable or upset by something that may have happened to them or other members of the school community online, or by something they may have done. If anything, online causes discomfort, concern, or distress this should be shared with an appropriate member of staff (via parents or tutors). Please refer to paragraph 10 below for further information on how to report concerns.

7.1.2 Students should avoid excessive or addictive online and digital behaviour.

7.1.3 Students are expected to inform parents/guardians of all social media platforms being used for personal use and for parents/guardians to check the appropriate age restrictions and privacy settings are in place and that the school is not being represented or brought into disrepute.

7.1.4 Students must be aware that that social media or online channels that can be identified as associated with school-aged students can attract unwelcome attention and can endanger accounts associated with these channels through follow-lists and related activity.

7.1.5 Only verified contacts should be added to friends/follower lists and caution should be exercised when communicating with contacts that are only known to you online (informing a member of staff responsible for online safety, via a parent if appropriate). Be aware that it is very easy to impersonate an account name online – check, before accepting and never accept from strangers.

7.1.6 Students should understand that being asked for secrecy by online contacts can support/encourage grooming and that, therefore, removing secrecy by sharing online experiences with friends and family can prevent online harm and abuse.

7.1.7 Students should be aware that people online may be untruthful about their identity, intentionally seek to cause them harm or spread violent or extremist views through radicalisation.

7.1.8 Those who seek to promote terrorism or religious extremism may attempt to contact or recruit young people via the Internet and such activity must be reported.

7.1.9 Students must be aware that entering online chats, forums and channels can expose the individual or school community to strangers.

7.1.10 While social media is not permitted for schoolwork without authorisation by the Director of Communications, the school expects profiles for its staff and students to be checked regularly and set to the highest levels of privacy for the benefit of its wider community.

7.2 Social Media

7.2.1 Social media channels should not be used:

- without adhering to school AUPs;
- unless with explicit, written authorisation; and
- without adhering to the school guidelines for public-facing online content below.

7.3 Public-facing online content

7.3.1 Public-facing activity is defined as activity on the internet or using channels that are outside of the school network, including so-called 'private' channels.

7.3.2 Any activity that is recognisably associated with the school, whether explicitly using the school name or not, is subject to our school AUPs.

7.3.3 Our school IT network is a protected environment for communication and collaboration in the course of its school provision and should be used in preference to public-facing channels wherever possible.

7.4 Mobile phones and portable electronic devices

7.4.1 Students may use mobile phones and portable electronic devices as outlined in the school Mobile Device Policy, Student Device Guidelines, and the Student Acceptable Use Policy.

7.4.2 If staff become aware of a breach of school AUPs, they may confiscate a student's personal device and should then pass it to the Director of Pastoral Care or Director of IT for investigation.

7.4.3 Staff and students should be aware that sharing of nudes is a particular problem for school-age children and should seek advice immediately from the Director of Pastoral Care/DSL if they suspect such behaviour and refer to the school safeguarding policy and KCSIE for further guidance.

7.5 Photography/Video recording/Audio recording/Publishing of content

7.5.1 Please refer to the school's AUPs and the Taking, Storing and Using Images of Students Policy.

8. Technical infrastructure

8.1 The school IT network, systems, and facilities are configured in such a way as to support a safe and secure environment in which to learn. Where possible our systems provide additional security and safety through single-sign-on and multi-factor authentication with intelligent monitoring.

8.2 It is, however, recognised that technical barriers can never entirely protect students from harmful content and that the same protection is not necessarily in place when using other networks, which reinforces the need to develop safe, responsible behaviour.

8.3 For instance, students at home or using mobile devices connected via mobile networks are not subject to school network filtering systems, though they are bound by the Student Acceptable Use Policy. There are no technical measures that can be put in place to prevent this and so the risks involved in accessing content via an unfiltered connection are addressed through developing safe, responsible behaviour and parents/guardians are recommended to put age-appropriate parental controls in place for students' personal data plans.

8.4 The schools' 1:1 device scheme (launched September 2020) is in force across the year groups- MIV to VI. The devices are covered by the same level of filtering and monitoring as they would be logged in when inside the school. Necessary device and application controls are applied to ensure a secure and safe experience for students which is continually reviewed as required.

8.5 Rules on how to use school IT facilities are set out in the school's AUPs, which staff and students are required to sign at the start of each school year. Any breach of these rules is dealt with in accordance with school behaviour policies and may lead to the withdrawal of IT facilities and, in the case of serious misconduct, may lead to disciplinary action.

9. Information security & safety

9.1 Network access – filtering and monitoring

9.1.1 Network access for all connected devices is logged and filters are in place to limit or block traffic where appropriate; this includes blocking illegal, potentially harmful sites, and decryption of secure websites (for the purposes of filtering and security). It should be borne in mind that this is not always technically possible, and methods of sidestepping school protections (VPNs etc.) are a constant possibility, despite being contrary to AUPs.

9.1.2 The school implements keyword and artificial intelligence filtering across a broad spectrum of categories including cyberbullying, self-harm and grief. Automatic block lists are updated daily by the system provider of the web filter, which ensures where possible that lists of illegal or potentially harmful websites are kept up to date, as well as manually blocking specific websites or applications that are considered harmful or inappropriate by the school. This is informed, in part, by the risk assessment required by the Prevent Duty.

9.1.3 The following categories are blocked across all year groups outside age-appropriate restrictions:

- **Adult Content:** Explicit content that may include violence or graphic content.
- **Chat/Messaging:** Websites that have their own instant messaging services.
- **Drugs:** Websites that provide info about alcohol and prescription or recreational drugs.
- **Gambling:** Anything that promotes betting or risky actions for a reward.
- **Games:** Websites that feature single or multiplayer online games without appropriate safeguarding. Games of strategy or other educational benefits such as chess may be permitted.
- **Hate:** Any content that hatefully targets another person or group.
- **Network Misuse:** Websites That Allow Anonymity, Hacking, Or Evasion.
- **Pornography:** Websites with sexually explicit content and nudity.
- **Search Engines (No Safe Search):** Google, Bing and Yahoo are **approved** with Safe Search
- **Social Media:** Media hosting communities with forums or communities that allow generated content and may be targeted for grooming.
- **Social Networking:** Sites used to create personal and professional relationships.
- **Streaming Media:** Sites that host video or audio content that can be watched or heard live.

9.1.4 It is recognised that there may be occasions when, for good educational reasons, students and staff may need to access content that is normally blocked. When this happens, a request may be submitted to the IT Service Desk for consideration.

9.1.5 The Director of IT reviews the internet filtering rules quarterly and consults with the Heads of Year and the Senior Management Team as necessary.

9.1.6 The school's internet filtering and monitoring systems provide information and alerts on students' network activity and behaviour that might constitute a safeguarding concern. The Director of Pastoral Care reviews this information daily and any potential concerns are delegated to the Heads of Year to investigate. The Director of Pastoral Care and Heads of Year agree on how potential safeguarding concerns are evaluated to ensure that they are addressed appropriately.

10. Reporting Concerns

10.1 If there is suspicion of a safeguarding concern including online activity, the policy for reporting concerns is outlined in the Safeguarding (Child Protection) Policy. If in any doubt, students and staff should consult a member of the safeguarding team, lists of whom are published in the *key contacts* section of the safeguarding policy.

10.2 For technical advice specific to online safety, without any immediate safeguarding concern, further advice can be sought from the IT Department at itservices@spgs.org, in person in the IT Office, or by dialling 020 7605 4860. In any of these cases, you should request:

- The Online Safety Officer – the Assistant Head Teaching & Learning (innovation), whose office can be found in 217 (also on 020 7605 1128 and giles.bennett@spgs.org).
- The Online Safety Coordinator – the Director of IT, whose office is in the IT Department (also on 020 7605 4862 and directorofit@spgs.org).
- The Director of Strategic Development – room 220 (also on 020 7605 4849 and strategicdevelopment@spgs.org).

Appendix 1: Information and support

- Teaching online safety in school - DfE guidance outlining how schools can ensure their students understand how to stay safe and behave online as part of existing curriculum requirements.

- UKCIS has recently published its Education for a connected world framework. Online safety is a whole school and college issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18.

- The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk

Organisation / Resource	What it does/provide
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including nudes and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
UKCIS	The UK Council for Internet Safety's website provides: · Sexting advice · Online safety: Questions for Governing Bodies · Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
BBC Webwise	A series of short films introducing topics in relation to using email, using the internet, using mobiles and keeping safe online.

Appendix 2: Online conferencing and collaboration (with other schools and organisations)

Platform
St Paul's has configured Zoom as an educational platform for its staff and students. In order to secure our channels for safe interaction, we have configured the following:

- All school email accounts (ending in @spgs.org) are brought into our educational licence and staff have access to Pro licences within this framework for the hosting of lessons etc.
- The school licence operates single-sign-on (SSO) for St Paul's account holders.
- Multifactor authentication is implemented for St Paul's staff and students.
- All meeting invitation links are password protected and the waiting room is enabled for safe admission to meetings on the platform.
-

In addition, the use of Microsoft Teams is now adopted as the preferred platform for online meetings and video conferences. Teams uses the same SSO system as other MS products and meets the school's digital safety requirements.

Recording Events
School policies should apply regarding recording:

- St Paul's, for example, has a *consent at the point of unmuting of cameras* policy where students and parents are aware that consent for recording is implicit when a student activates their camera and students will be aware that a session is being recorded by the 'record icon' in the top left of their screen.
- Under no circumstances should students record or capture recordings of school events. Students must be made aware that screen grabs and screen captures are considered a gross breach of privacy and school rules and re-broadcast of material by students to, for example, social media is forbidden under any circumstances.
- Staff are asked to exercise their judgment in the download of any material that may be recorded (accessible at St Paul's only to the Host who has chosen to select record and the designated safeguarding lead team). Any use of such material should only be made on request to the event organiser and subject to the participating schools' privacy, safeguarding and data protection policies. At St Paul's, for example, no material will be published beyond the school community without express permission from participants and their parents via our Communication Department.
- Attendance at Zoom events by students from other schools.
- Our bricks-and-mortar mode of operation also allowed for Year 11, 12 and 13 students to attend talks and events without a member of staff from their own school. Once at St Paul's, they are supervised by our staff at all times. The following guidelines should apply in this situation:
- It needs to be clear who is hosting the event from St Paul's.
-
    - Year 11, 12 and 13 students from other schools can attend Zoom events without an accompanying teacher if it is organised through their school and the partnerships team is aware.
    - A list of students attending should be provided in advance and students asked to add their school to their display name.
    - Students must sign in using their school email address. The host will need to make sure that the domain is added to the authenticated user list.
    - At least one member of staff from the partner school(s) must be invited to the meeting.
    - Students from partner schools can be sent to a breakout room with our students but the host should monitor these regularly, this includes for 1:1 mentoring or buddying. As stated above, staff should not be alone with students from another school.
    - Students from partners schools will need to be aware of our Zoom etiquette guidelines.
    - 1:1 Meetings between our staff and students from other schools (such as interview preparation).
    - Our usual 1:1 policy applies - recording the meeting with names, disabling the waiting room, inviting another member of staff to the meeting who can drop-in.

- Partner schools will need to be made aware of, and agree to, our 1:1 policy (especially recording). They must make their students aware that sessions are recorded.
- Students must sign in using their school email address. Staff will need to make sure that the domain is added to the authenticated user list.
- At least one member of staff from the partner school must be invited to the meeting and they should be encouraged to visit the meeting at some point.
- The partnerships and/or HE team must be aware of all such meetings.

Collaboration
When collaborating with other schools, we adopt an analogy between our *bricks & mortar* model of operation with our *network & ether* model:

- Schools joining our platform should decide at their own discretion the appropriate number of staff to supervise students from their own school. If each school would like one of their own staff to be present for all breakout sessions that their students are attending, as well as other sessions, this should be taken into account.
- Staff and students should join meetings logged in using their school email accounts. St Paul's operates an 'authenticated users' only policy and will open collaborative meetings to school domain email addresses only plus any authenticated guests.
- Meetings will be established with a 'waiting room' and visiting staff will be admitted first. On admission, visiting staff will be given co-host permissions in order to manage participants from their school and must only admit students from their own schools to the meeting from the waiting room.
- Hosts and co-hosts have the ability to record meetings or breakout rooms that they attend but it is the policy at St Paul's that only one-to-one meetings between a member of staff and a student should be recorded (and held for 120 days).
- We do not allow one-to-one meetings in our collaborative events between staff from one school and students from another. The waiting room, and breakout room allocations, should be managed carefully to avoid this. If a member of staff finds themselves in this position, they should remove the student and ask them to rejoin (at which point they can be re-admitted from the waiting room). This can be managed from the participants' pane.

1:1 Meetings (or 1:2, 1:3) between our students and a student from another school (such as buddying or mentoring)
These should take place only as part of a school-organised project and must be overseen by a member of staff. The following guidelines would apply:

- Written parental permission obtained for all parties (partner schools to manage this for their students and confirm).
- An email address for the DSL is provided.
- All meetings recorded and labelled 1:1 <name><name>.
- A responsible adult, usually a parent, undertakes to be present and supervise each person in the meeting but is not part of the session.
- Meetings are always at a pre-arranged time which does not vary. The safeguarding team should have a list of all meetings and be able to drop in therefore the waiting room needs to be disabled.
- Staff from both schools have access to drop into the meet at any time.

Our students attending webinars and events at other schools

- There should be due diligence in advance in researching the provider and ascertaining what supervision is in place for the event. We should know:
    - Who is hosting?
    - Are there any 1:1 sessions? These should not be between an adult and our students.
    - Can third parties contact our students during the event?
    - Is there a safeguarding lead?
    - Have any visiting speakers been checked (for example, radicalisation content)?
- Students should join with their school email address only and the process would generally mirror our advice for collaboration above.
- There should be a way for staff to communicate with our own students in the event of inappropriate content. At present email is likely to be the best channel for this and students

should be asked to enable notifications in email as well as being briefed on leaving the meeting if they feel uncomfortable.

- Senior students:
    - Allowed with remote supervision.
    - Supervising nominated member of staff (but not attending).