



ST PAUL'S
GIRLS' SCHOOL

Online Safety Policy

Published September 2026

Document owner	Deputy Head (Safeguarding & Inclusion)/DSL
Approved by	Education Committee
Date published	September 2026 – pending final approval
Review cycle	Biennially
Next review date	September 2028
Availability	School website; staff portal; student portal; parent portal

Legal framework

- Keeping Children Safe in Education 2026
- Prevent Duty
- Data Protection Act 2018
- UK GDPR
- Online Safety Act 2023
- Data (Use and Access) Act 2025

Availability of this policy

A copy of this policy may be downloaded from our [website](#) or is available on request from the school office, St Paul's Girls' School, Brook Green, London, W6 7BS (tel: 0207 603 2288). This policy can be made available in large print or other accessible format if required.

Who this policy applies to

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy

- “staff” includes teaching and non-teaching staff, governors, and volunteers
- “parents” includes students’ carers and guardians
- “visitors” includes anyone else who comes to the school

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 personal devices in all their forms.

Other relevant school policies

The school recognises that digital and online safety is an extension of its 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
- Data Protection policy
- Behaviour policy (including rewards and sanctions)
- Anti-bullying policy
- Student ICT Acceptable Use policy (AUP)
- Staff ICT Acceptable Use policy (AUP)
- Device policy
- Cybersecurity policy
- Generative AI policy
- Staff Code of Conduct
- Mobile Phone policy
- Taking, Storing and Using Images of Students policy
- Mental Health & Wellbeing policy
- Online Resource Approval Procedure
- School PSHE/RSE programme

Table of Contents

Legal framework	1
Who this policy applies to.....	2
What this policy is for	2
Other relevant school policies	2
Aims and objectives.....	4
Risk	4
Overview	5
Delivery.....	5
School/parent partnership	6
Visitors with access to the school network	6
Online collaboration, events and remote learning	6
Online activity	6
Photography/video recording/audio recording/publishing of content	7
Filtering & monitoring.....	7
Reporting concerns	7
Appendix 1: Roles and responsibilities in relation to online safety.....	8
Governing Body	8
Senior Leaders.....	8
Online Safety Officer (Director of IT)	8
All staff	8
All students	8
Parents/Guardians.....	8
Appendix 2: Online events, conferencing & collaboration.....	9
Purpose	9
Platform standards.....	9
Online Events and Collaboration	9
General Requirements	9
Events Involving External Participants.....	9
Student Collaboration with Other Schools and Partners	9
One-to-One and Small Group Meetings	10
Recording and Retention.....	10

Aims and objectives

1.1 St Paul's Girls' School (the 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 The school sets out to enable the delivery of teaching and learning within a safe and secure digital environment with policies and processes that encourage online behaviour to reflect the school culture as a whole.

1.3 The school recognises 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 the school recognises that emerging technologies also bring risks and potential dangers.

1.4 The school aims to:

- Protect students online
- Educate students
- Maintain effective technical safeguards
- Promote responsible behaviour
- Support parents
- Provide reporting mechanisms.

Risk

2.1 The breadth of issues classified within online safety is considerable, but can be categorised into the following areas of risk **often referred to as the 4 Cs**:

- **Content**: harm that can arise from exposure to inappropriate, misleading, distasteful, extremist, radicalising or illegal content
- **Contact**: harm that can arise from interactions with other individuals online or with generative AI applications that simulate this e.g. peer to peer pressure, commercial advertising and adults posing as young children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct**: harm that can arise from how young people behave online e.g. making, sending and receiving explicit images. This includes consensual and non-consensual sharing of self-generated intimate images and/or videos including those generated by AI e.g. deepfakes, sharing other explicit images and online bullying
- **Commerce**: harm that can arise as a result of financial traps, scams or gambling.

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

- **Privacy, security and fraud risks**, including oversharing personal information, identity theft, phishing, data misuse and unauthorised access to accounts or data
- **Inappropriate contact and exploitation**, including grooming, coercion and abuse by strangers or known individuals
- **Cyberbullying and online harassment**, including image-based abuse and unwanted communications
- **Exposure to harmful content**, including sexual, violent, self-harm, suicide-related, extremist, terrorist or hate-related material

- **Misinformation and manipulation**, including disinformation, conspiracy narratives, deepfakes and other AI-generated content intended to mislead or radicalise
- **Illegal or unethical online activity**, including copyright infringement, plagiarism and unauthorised downloading or sharing of content
- **Excessive or addictive use of technology**, which may negatively affect wellbeing, learning and social or emotional development
- **Risks arising from emerging technologies**, including artificial intelligence, which may contribute to or amplify any of the risks above

2.3 In response to these risks, the school has developed a multi-layered approach that includes clear responsibilities, education and training, and robust technical controls; see below.

Overview

The school's approach to online safety is built on several key elements:

- **Governance and oversight:** The Online Safety Committee provides strategic oversight, monitoring and assurance in relation to online safety. The IT Steering Group retains oversight of the school's wider digital infrastructure and cybersecurity arrangements. Governors provide strategic oversight and receive assurance regarding the effectiveness of the school's online safety arrangements, including involvement in the annual review of filtering and monitoring
- **Shared responsibility:** Online safety is a partnership between the school, students and parents. All users must comply with the relevant ICT Acceptable Use Policies and expected standards of behaviour. Staff responsibilities are outlined in Appendix 1
- **Beyond the school environment:** The school works with parents to promote safe use of technology outside school, recognising that personal devices and home networks are beyond its direct control
- **Technology and network security:** The school maintains secure systems and uses filtering, monitoring and other technical controls (Appendix 2), while reviewing emerging technologies and managing personal data appropriately
- **Devices and online resources:** School-managed devices and approved online resources support safeguarding, educational suitability and compliance with data protection requirements
- **Education and awareness:** Ongoing education and training for students, staff, parents and governors promote safe, responsible and effective use of technology.

Delivery

4.1.1 The school provides age-appropriate online safety education for students and regular training for staff through the curriculum, PSHE, assemblies, inductions, INSET, refresher training and other development opportunities including external specialists. Training addresses current and emerging online safety risks.

4.1.2 Online safety education and training form part of the school's whole-school safeguarding approach and are embedded within induction, staff development and curriculum planning.

4.1.3 All online resources used for schoolwork are subject to the Online Resource Approval process. As students develop greater independence online, they are taught how to evaluate content, act safely and responsibly, and report concerns relating to inappropriate content, safeguarding or security.

4.1.4 Online safety concerns and emerging risks are communicated regularly to staff. Staff raise any concerns with the Deputy Head (Safeguarding & Inclusion)/DSL, Deputy Head (Pastoral) or Online Safety Officer.

School/parent partnership

4.2.1 Parents are expected to support the school's online safety approach by supervising technology use outside school and promoting safe, age-appropriate online behaviour. The school provides guidance and updates through a range of communication channels.

4.2.2 The school and parents work in partnership to help students navigate online risks, respond appropriately to harmful content and raise concerns when necessary.

4.2.3 Breaches of this policy or related school policies may result in disciplinary action, regardless of whether incidents occur on or off the school network.

Visitors with access to the school network

4.3.1 The school is a mobile phone-free environment; visitors may request permission to use their device from their hosting member of staff, who will seek the necessary internal approvals. Access to the school network for visitors should be restricted to only that which is applicable and appropriate.

4.3.2 Visitors are able to generate a unique WiFi key to access the Visitor WiFi. As part of their registration for this, they must agree to the Visitor Acceptable Use policy which is published on the iPads as part of the signing in process. The AUP outlines that devices will be monitored, outlines the permitted use of the systems and makes clear the activities that are not permitted.

Online collaboration, events and remote learning

4.4.1 The provision of remote learning for curriculum teaching is preserved for exceptional circumstances.

4.4.2 Online conferencing is a method for schools to collaborate and run events. Details of the school's approach to this can be found in Appendix 2.

4.4.3 Small or one-to-one online meetings are subject to the school's One-to-One Online Meetings (1:1) policy, see Appendix 2.

Online activity

5.1 Students must use the school network for online access during the school day and comply with the school policies concerning use of mobile phones and online activity.

5.2 Students are encouraged to seek support from a member of staff if they encounter online content or behaviour that causes concern, distress or poses a safeguarding risk. Reporting procedures are outlined in Section 6.

5.3 The school promotes a culture in which students feel able to discuss concerns about their own or others' online behaviour, including excessive or unhealthy use of technology.

5.4 The school does not use social media for teaching or communication. Students must not create social media accounts, websites, channels or content that appear to represent the school or use school branding without authorisation. They should use social media responsibly, follow age restrictions and privacy settings, and ensure their online behaviour does not bring the school into disrepute.

5.5 Students should exercise caution when communicating online, recognise the risks of grooming, impersonation, exploitation and extremist content, and report any concerns to a trusted adult.

5.6 Participation in online communities may expose students to unknown individuals and harmful content. Students should engage responsibly and avoid sharing personal information unnecessarily.

5.7 Students and staff should be aware that images, videos and other content may be manipulated or generated using artificial intelligence. Any safeguarding concerns, including the creation, possession or sharing of indecent images, must be reported immediately in accordance with school procedures.

5.8 Students must understand that certain online behaviours may constitute criminal offences under UK law. These include, but are not limited to: cyberflashing; sending threatening, abusive or knowingly false communications; creating, requesting or sharing intimate deepfake images without consent; sharing content that encourages serious self-harm or suicide; and unlawful access to, misuse of or disclosure of personal data. Further information on cybersecurity awareness, including phishing, passwords and multi-factor authentication (MFA), is contained within the school's Cybersecurity Policy.

Photography/video recording/audio recording/publishing of content

5.9 Please refer to the school's AUPs, Appendix 2, 'Online events, conferencing & collaboration'. and the Taking, Storing and Using Images of Students policy.

Filtering & monitoring

The school maintains filtering and monitoring systems for all devices connected to its network. Network activity is logged, and technical controls are used to restrict access to illegal, harmful or inappropriate content, including the inspection of encrypted traffic where technically feasible and lawful. While these measures reduce risk, the school recognises that no filtering system can provide complete protection and that users may attempt to circumvent controls through methods such as VPNs, contrary to the ICT Acceptable Use Policies.

Filtering arrangements incorporate automated blocklists, keyword monitoring and AI-assisted detection across a range of safeguarding categories, including cyberbullying, self-harm and extremist content. These controls are regularly updated by the provider and supplemented by school-specific restrictions, informed where appropriate by safeguarding and Prevent risk assessments.

The school operates age-appropriate filtering and monitoring arrangements. Where access to otherwise restricted content is required for legitimate educational purposes, staff or students may request approval through the IT Service Desk.

Filtering and monitoring systems generate alerts and information relating to potential safeguarding concerns. Filtering and monitoring reports are reviewed regularly by safeguarding, pastoral and IT staff to identify trends and potential concerns. The Deputy Head (Safeguarding & Inclusion)/DSL, Deputy Head (Pastoral) and Heads of Year work together to assess concerns and determine any necessary action.

The effectiveness of the school's filtering and monitoring arrangements is reviewed at least annually by the Online Safety Committee and responsible Governor. Records of reviews, findings and actions taken are retained, and appropriate assurance is provided to relevant governors and senior leaders regarding the effectiveness of the school's arrangements and any safeguarding risks identified.

Reporting concerns

6.1 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 the Deputy Head (Safeguarding & Inclusion)/DSL, or a member of the safeguarding team, lists of whom are published in the key contacts section of the Safeguarding (Child Protection) policy.

6.2 For matters relating to misuse of the network, without any immediate safeguarding concern, this should be referred to the Online Safety Officer.

Appendix 1: Roles and responsibilities in relation to online safety

All staff, governors and volunteers have a duty to protect children from abuse and to report matters of concern to the Designated Safeguarding Lead (DSL) in line with the Safeguarding (child protection) policy.

Governing Body

- Provides strategic oversight of online safety
- Ensures appropriate filtering and monitoring systems are in place and reviewed regularly
- Receives assurance from senior leaders that online safety and safeguarding arrangements are effective. These feed through from the IT Steering group which oversees the school's network and digital infrastructure
- Approves and periodically reviews this policy
- Ensures sufficient resources are available for online safety education, training and technical safeguards.

Senior Leaders

Deputy Head (Safeguarding & Inclusion)/DSL (see the school's safeguarding policy for the full list of responsibilities for this role)

- Lead for child protection, student and online safety including those presented by emerging technologies
- Understands the filtering and monitoring arrangements and the associated safeguarding risks and conducts an annual review of these whilst maintaining evidential records
- Receives assurance that appropriate cybersecurity controls are in place to protect student data and understands any associated safeguarding risks.

Deputy Head (Pastoral)

- Oversees PSHE/RSE curriculum, including online safety education
- Reviews filtering/monitoring alerts and helps coordinate pastoral responses.

Online Safety Officer (Director of IT)

- Oversees technical infrastructure security and advises on digital and technical safety matters
- Provides specialist advice, updates and technical input to online safety training for staff and parents
- Manages filtering and monitoring systems, provides reports to safeguarding teams
- Investigates network misuse.

All staff

- Must follow the Online Safety policy, Staff Code of Conduct, and AUPs
- Promote responsible behaviour and escalate concerns.

All students

- Adhere to the content of this policy and the student AUPs
- Engage with the school programme of education and training for online safety
- Report unacceptable and inappropriate behaviour, including the behaviour of others.

Parents/Guardians

- Support the school's online safety expectations
- Monitor their child's use of technology and online services outside school
- Use parental controls and privacy settings where appropriate
- Raise any online safety concerns with the school.

Appendix 2: Online events, conferencing & collaboration

Purpose

The school recognises that online meetings, remote collaboration and virtual events are an established part of education. All online activity involving students must meet the same safeguarding standards as activities conducted in person. Staff are responsible for ensuring that appropriate supervision, safeguarding measures and technical controls are in place.

Platform standards

- Microsoft Teams is the default platform due to Single Sign On integration and safety controls
- Other platforms (e.g., Zoom, Google Meet) may be used for external events if the following are applied:
 - Account security: only @spgs.org and approved accounts permitted; staff use Pro licences with Multi-Factor Authentication
 - Meeting controls: all links must be password-protected
 - Access management: waiting room enabled; staff admit only their own students
 - Student privacy: student chat is disabled
- A *Student Online Meetings* Team has been set up and must be used for all 1:1 and small-group meetings. This is overseen by the DSL and Online Safety Officer and holds the recording of any online session that has been recorded
- Only school-authorised accounts can be used.

Online Events and Collaboration

General Requirements

- All online meetings, events and collaborations involving students must meet the same safeguarding standards as equivalent in-person activities
- School-approved platforms, authenticated accounts and school email addresses must be used
- Meetings should be planned in advance, appropriately supervised and proportionately risk-assessed where standard safeguards cannot be applied
- Ad hoc student meetings with external participants are not permitted.

Events Involving External Participants

- Staff must ensure that external organisations, speakers and event hosts are suitable and have been vetted in accordance with safeguarding requirements where appropriate
- Appropriate staff supervision and safeguarding arrangements must be in place, including clear reporting procedures and designated safeguarding contacts
- External participants must not have unsupervised or unrestricted contact with students.

Student Collaboration with Other Schools and Partners

- Collaboration with students from other schools may only take place as part of an approved school activity and under staff oversight
- Appropriate safeguarding information must be shared between participating schools, including DSL contact details where required
- Parents should be informed where appropriate and students should receive safeguarding guidance before participation.

One-to-One and Small Group Meetings

- One-to-one or small-group online meetings should only take place where necessary and must use approved school systems
- Appropriate safeguarding measures may include advance scheduling, staff oversight, recording in accordance with school procedures, involvement of safeguarding staff where appropriate, and risk assessment where required
- For all 1:1 meetings, the Deputy Head (Safeguarding & Inclusion)/DSL and the Deputy Head (Pastoral) must also be invited, even if they are not expected to attend.

Recording and Retention

- Recordings must be managed in accordance with school procedures, with participants informed in advance and access restricted to authorised staff
- Students must not record or capture meetings without permission
- Exceptions may be authorised by the Deputy Head (Safeguarding & Inclusion)/DSL or Deputy Head (Pastoral) where recording would be inappropriate.