ST PAUL'S CATHEDRAL SCHOOL

Acceptable Use of ICT Policy (Pupils)

Academic Year 2025-2026

Aims and Principles

St Paul's Cathedral School is a Christian, co-educational community which holds to the values of love, justice, tolerance, respect, honesty, service and trust in its life and practice, to promote positive relationships throughout the school community and where the safety, welfare and emotional well-being of each child is of the utmost importance.

The school aims to instil a love of learning through a broad curriculum. It aims to give each pupil the opportunity to develop intellectually, socially, personally, physically, culturally and spiritually. All pupils are encouraged to work to the best of their ability and to achieve standards of excellence in all of their endeavours.

Through the corporate life of the school, and through good pastoral care, the school encourages the independence of the individual as well as mutual responsibility. It aims to make its pupils aware of the wider community, espouses the democratic process and encourages a close working relationship with parents and guardians.

1 Aims

1.1 This is the acceptable use of ICT policy for pupils of SPCS (the school).
1.2 The aims of this policy are as follows:

1.2.1 to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

1.2.2 to safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

(a) exposure to potentially illegal, harmful or inappropriate content (such as pornographic, racist, extremist or offensive materials);
(b) the sharing of personal data, including images;
(c) inappropriate online contact or conduct, including sexual harassment;
(d) cyberbullying and other forms of abuse; and
(e) online challenges and online hoaxes.

1.2.3 to minimise the risk of harm to the assets and reputation of the school;
1.2.4 to help pupils take responsibility for their own safe use of technology;
1.2.5 to ensure that pupils use technology safely and securely and are aware of both external and peer group risks when using technology;
1.2.6 to prevent the unnecessary criminalisation of pupils; and
1.2.7 to help to promote a whole school culture of openness, safety, equality and protection.

1.3 This policy forms part of the school's whole school approach to promoting child safeguarding and wellbeing, which involves everyone in the school and seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

2 Scope and application

2.1 This policy applies to the whole school including the Early Years Foundation Stage (EYFS) – our Reception – and Boarders.

2.2 This policy applies to pupils using or accessing the school's technology whether on or off school premises, or using their own or others' technology in a way which affects the welfare of other pupils or any member of the school community or where the culture, reputation or orderly running of the school are put at risk.

2.3 Parents are encouraged to read this policy with their child. The school actively promotes the participation of parents to help the school safeguard the welfare of pupils and promote the safe use of technology.

3 Regulatory framework

3.1 This policy has been prepared to meet the school's responsibilities under:
3.1.1 Education (Independent school Standards) Regulations 2014;
3.1.2 EYFS statutory framework for group and school-based providers (DfE, November 2024);];
3.1.3 Education and Skills Act 2008;
3.1.4 Childcare Act 2006;
3.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR); and
3.1.6 Equality Act 2010.
3.2 This policy has regard to the following guidance and advice:
3.2.1 Keeping children safe in education (DfE, September 2024);
3.2.2 Preventing and tackling bullying (DfE, July 2017);
3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (DfDCMS) and UK Council for Internet Safety (UKCIS), March 2024);

3.2.4 Technical guidance for schools in England (Equality and Human Rights Commission, July 2024);
3.2.5 Relationships education, relationships and sex education and health education guidance (DfE, September 2021);
3.2.6 How can we stop prejudice based bullying in schools? (Equality and Human Rights Commission);
3.2.7 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);
3.2.8 Searching, screening and confiscation: advice for schools (DfE, September 2022):
3.2.9 Mobile phones in schools (DfE, February 2024); and
3.2.10 Behaviour in schools: advice for headteachers and school staff 2022 (DfE, February 2024).
3.3 The following school policies, procedures and resource materials are relevant to this policy:
3.3.1 Good Behaviour Policy;
3.3.2 Anti-Bullying Policy;
3.3.3 Online Safety Policy;

3.3.5 Safeguarding Policy And Child Protection Policy Procedures;
3.3.6 Relationships Education and Relationships and Sex Education Policy;
3.3.8 Equal Opportunities Policy

4 **Publication and availability**

4.1 This policy is available in hard copy on request.
4.2 A copy of the policy is available for inspection from the school office during the school day.
4.3 This policy can be made available in large print or other accessible format if required.

5 **Definitions**

5.1 Where the following words or phrases are used in this policy:

5.1.1 References to **Staff** includes all those who work for or on behalf of the school, regardless of their employment status, including contractors, supply staff, volunteers and Governors unless otherwise indicated.

5.2 The school will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology)**. This policy relates to all technology, computing and communications devices, network hardware and software, and services and applications associated with them including:

5.2.1 social networking, micro blogging and other interactive websites;
5.2.2 the internet;
5.2.3 email and school messaging platforms including Microsoft Teams
5.2.4 generative artificial intelligence technology/tools;
5.2.5 electronic communications;
5.2.6 mobile phones and smart technology;
5.2.7 wearable technology;
5.2.8 desktops, laptops, netbooks, tablets / phablets, chromebooks;
5.2.9 personal music players;
5.2.10 devices with the capability for recording and / or storing still or moving images;
5.2.11 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;
5.2.12 webcams, video hosting sites (such as YouTube);
5.2.13 gaming sites;
5.2.14 virtual learning environments (such as Microsoft Teams);
5.2.15 SMART boards, display screens;
5.2.16 other photographic or electronic equipment e.g. GoPro devices; and

5.2.17 devices which allow sharing services offline (such as Apple's AirDrop).

6 **Responsibility statement and allocation of tasks**

6.1 The Board of Governors has overall responsibility for all matters which are the subject of this policy.
6.2 To ensure the efficient discharge of its responsibilities under this policy, the Board of Governors has allocated the following tasks:

Task	**Allocated To**	**Review timing/frequency**
Keeping the policy up to date and compliant with the law and best practice	Deputy Head (DSL)	annual
Monitoring the use of technology across the school, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change	IT Manager/Head of IT	Monitoring is on a rolling basis, policy review at least annually
Monitoring the implementation of the policy, including the record of incidents involving the use of technology and the logs of internet activity and sites visited, relevant risk assessments and any action	DSL Chairs IT monitoring/filtering group (Director of Finance and Operations, DSL, IT Manager, Head of IT)	Termly
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the UK GDPR	Director of Finance and Operations	As required and at least termly
Seeking input from interested groups (such as pupils, staff, parents) to consider improvements to the school's processes under the policy	Deputy Head Academic	Annually
Formal Annual Review	DSL	Annually

7 **Safe use of technology**

7.1 We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.
7.2 The school will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. The safe use of technology is integral to the school's curriculum. Staff are aware that technology can be a significant component in many safeguarding and wellbeing issues and pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.
7.3 Pupils may find the following resources helpful in keeping themselves safe online:

7.3.1 http://www.thinkuknow.co.uk/
7.3.2 http://www.childnet.com/young-people
7.3.3 https://www.childnet.com/resources/smartie-the-penguin
7.3.4 https://www.childnet.com/resources/digiduck-stories
7.3.5 https://www.saferinternet.org.uk/advice-centre/young-people
7.3.6 http://www.childline.org.uk/Pages/Home.aspx
7.3.7 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

7.4 Please see the school's *Online Safety Policy* for further information about the school's online safety strategy.

8 **Internet and email/electronic communication systems**

8.1 The school provides internet, intranet access and, in Year 7 and above, an email/electronic communication system ie. Googleclassroom, to pupils to support their academic progress and development.
8.2 Pupils may only access the school's network when given specific permission to do so. All pupils will receive guidance on the use of the school's internet and, where accessible, email/electronic communication systems. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff. Pupils are given individual user names and passwords to access the school's intranet and email system and these details must not be disclosed to any other person.
8.3 No laptop or other mobile electronic device may be connected to the school network without the consent of the Head of ICT. The use of any device connected to the school's network will be logged and monitored by the ICT Department.
8.4 For the protection of all pupils, their use of email/electronic communication system and of the internet will be monitored by the school. Pupils should remember that even when an email/electronic message or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

9 **School rules**

9.1 Pupils **must** comply with the following rules and principles:
9.1.1 access and security (Appendix 1);
9.1.2 communicating on or off-line using devices, apps, platforms and email (Appendix 2);
9.1.3 use of mobile electronic devices and smart technology (Appendix 3);
9.1.4 photographs and images (including the consensual and non-consensual sharing of nude and semi-nude images and videos (Appendix 4);
9.1.5 Online sexual harassment (Appendix 5); and
9.1.6 harmful online challenges and hoaxes (Appendix 6).

9.2 The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

9.3 These principles and rules apply to all use of technology in school and at home, whether during or outside school.

10 **Procedures**

10.1 The way in which pupils relate to one another online can have significant impact on the school's culture. Pupils are responsible for their actions, conduct and behaviour when using

technology at all times. Even though online space differs in many ways, the same standards of behaviour are expected online as apply offline. Use of technology should be safe, responsible and respectful to others and legal. If a pupil is aware of misuse by other pupils they should talk to a teacher about it immediately.

10.2 Any misuse of technology by pupils will be dealt with under the school's Good Behaviour Policy. Incidents involving the misuse of technology which are considered to be of a safeguarding nature will be dealt with in accordance with the school's Safeguarding and Child Protection Policy and procedures, rather than the school's Good Behaviour Policy.

10.3 Pupils must not use their own or the school's technology to bully others. Bullying incidents involving the use of technology, including cyberbullying, prejudiced-based bullying and discriminatory bullying, will be dealt with under the school's Anti-Bullying Policy. If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the school's Anti-Bullying Policy for further information about cyberbullying and e-safety, including useful resources.

10.4 The school has adopted a zero tolerance approach to sexual violence and sexual harassment – it is never acceptable and it will not be tolerated. Incidents of sexual violence or sexual harassment will not be dismissed as merely "banter" or "just having a laugh", "boys being boys" or "girls being girls", as this can lead to the creation of a culture of unacceptable behaviours and an unsafe environment for children and, in worst case scenarios, a culture that normalises abuse.

10.5 Sexual harassment, in the context of this policy, means "unwanted conduct of a sexual nature" and the school recognises that this can occur both online and offline. Pupils must not therefore use their own or the school's technology to sexually harass others at any time, whether during or outside of school. Incidents of sexual harassment involving the use of technology will be dealt with under the school's behaviour and discipline and safeguarding policies. If a pupil thinks that they might have been sexually harassed or that another person is being sexually harassed, they should talk to a teacher about it as soon as possible.

10.6 The school recognises that children's sexual behaviour exists on a wide continuum ranging from normal and developmentally expected to inappropriate, problematic, abusive and violent. Problematic, abusive and violent sexual behaviour is developmentally inappropriate and may cause developmental damage. Such behaviour can be classed under the umbrella term "harmful sexual behaviour" and the school is aware that this can occur online and/or face-to-face and can also occur simultaneously between the two.

10.7 Any reports of sexual violence or sexual harassment will be taken extremely seriously by the school and those who have been victim to such abuse will be reassured, supported and kept safe throughout. No pupil should ever be made to feel that they have created a problem or feel ashamed for reporting their concern. Pupils should be aware that teachers may not be able to provide an assurance of confidentially in relation to their concern as information may need to shared further (e.g. with the school's Designated Safeguarding Lead) to consider next steps. See Appendix 5 for further information.

10.8 The Designated Safeguarding Lead takes lead responsibility within the school for safeguarding and child protection, including online safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the school's child protection procedures (see the school's *Safeguarding and Child Protection Policy*). If a pupil is worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must tell a member of staff about it as soon as possible.

10.9 The school is also aware of the risks of radicalisation and understands that this can occur through many different methods (including social media or the internet. In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme in accordance with the school's *Safeguarding and Child Protection Policy*. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

10.10 **Cybercrime:**

1. 10.10.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber-dependent' (crimes that can be committed only by using a computer).
2. 10.10.2 Cyber-dependent crimes include:
    1. (a) Unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;
    2. (b) Denial of service (DoS or DdoS) attacks or 'booting', which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and
    3. © Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offences, including those above.
3. 10.10.3 The school is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber dependent crime.
4. 10.10.4 Any concerns about a pupil in this area will be referred to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead will then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing.

10.11 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Head of Pre-prep (where Pre-prep pupils or staff are involved) or the Deputy Head in the case of Prep-related incidents. The matter will be recorded centrally by the Deputy Head.

11 **Generative Artificial Intelligence**

11.1 The school recognises the increasing presence of generative artificial intelligence (AI) technology. Although generative AI is not new, recent advances mean this technology is easily available to pupils to produce AI-generated content such as text, audio, code, images and video simulations.

11.2 **AI should not be used at school or for Prep (homework), without specific permission from the teacher.** When using any generative AI technologies pupils are expected to consider the following:

11.2.1 AI and human intelligence are not the same: AI tools do not understand what they produce or the impact the generated content may have;

11.2.2 sometimes AI tools will generate answers that sound plausible but they may not be correct;

11.2.3 content produced may perpetuate harmful biases and stereotypes and may not be age-appropriate;

11.2.4 over-reliance on these tools will reduce opportunities to improve research skills, writing and critical thinking;

11.2.5 AI tools store and learn information submitted to them so personal data should never be entered;
11.2.6 if teachers indicate that pupils are permitted to use generative AI technologies in their work, pupils must observe all related instructions and guidance; and
11.2.7 submitting work produced in whole or part by AI without proper referencing or acknowledging use of AI may be considered cheating/plagiarism and inappropriate use of AI.

11.3 Any misuse or inappropriate use of AI technologies by pupils will be addressed in accordance with the school's Good Behaviour Policy and disciplinary procedures.

11.4 The school may implement measures to ensure the safe and appropriate use of AI technologies within its network. These measures may include monitoring AI activities, restricting access to certain AI systems, or providing guidelines and restrictions on the use of specific AI applications.

12 **Sanctions**

12.1 Where a pupil breaches any of the school rules, practices or procedures set out in this policy or the appendices, the Board of Governors has authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the school's Good Behaviour Policy including, in the most serious cases, permanent exclusion. Other sanctions might include: increased monitoring procedures; withdrawal of the right to access the school's internet and email / electronic communication facilities; detention, negatives. Any action taken will depend on the seriousness of the offence.

12.2 Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy and the school's Good Behaviour Policy.

12.3 If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 5 and 6 for more information on photographs and images.

12.4 The school reserves the right to charge a pupil or their parents for any costs incurred to the school as a result of a breach of this policy.

13 **Training**

13.1 The school ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that all staff, including supply staff, volunteers and Governors;

- understand what is expected of them by this policy; and
- have the necessary knowledge and skills to carry out their roles; and
- are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

12.1 Staff training is regularly updated and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and / or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. This training may be in addition to the regular safeguarding and child protection (including online safety) updates are required at induction and at least annually thereafter.

13.3 The level and frequency of training depends on the role of the individual member of staff.

13.4 The school maintains written records of all staff training.

14 **Risk Assessment**

14.1 The school recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The school will carry out regular, and at least annual, reviews of its approach to online safety supported by risk assessment which consider and reflect the risks faced by its pupils.

14.2 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

12.1 The format of risk assessment may vary and may be included as part of the school's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the school's approach to promoting pupil welfare will be systematic and pupil focused.

14.4 The Deputy Head and Head of Pre-prep have overall responsibility for ensuring that matters which affect pupil welfare in the Prep and Pre-prep respectively are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

14.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Deputy Head, who may delegate other members of staff to carry out the particular assessments.

15 **Record keeping**

15.1 All records created in accordance with this policy are managed in accordance with the law and the school's policies that apply to the retention and destruction of records. The Director of Finance and Operations is our school Data Controller.

15.2 All serious incidents involving the use of technology will be logged by the DSL

15.3 The information created in connection with this policy may contain personal data. The school's use of this personal data will be in accordance with data protection law. The school has published privacy notices on its website which explain how the school will use personal data. The school's approach to data protection is set out in the school's data protection policies and procedures. In addition, staff must ensure that they follow the school's data protection policies and procedures when handling personal data created in connection with this policy.

16 Version control

Date of adoption of this policy:	16th January 2025
Date for next review of this policy:	January 2026
Policy owner (SMT):	DSL and Deputy Head, Caroline Heylen
Policy owner (Governor):	Chair of Curriculum and Standards Committee, Andrew Da Silva

Appendix One

Access and security

1 Access to the internet from the school's computers and network must be for educational purposes only.

2 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the school's or any other computer system, or any information contained on such a system.

3 No laptop or other mobile electronic device may be connected to the school network without the consent of the ICT Manager.

4 The use of cellular data (e.g. GPRS, 3G, 4G, 5G etc) to access the internet while pupils are on school premises or otherwise in the care of the school is prohibited for all pupils~~,~~ as pupils are unable to benefit from the school's filtering and anti-virus software.

5 Passwords protect the school's network and computer system. **You must not let anyone else know your password.** If you believe that someone knows your password you must change it immediately.

6 You must not attempt to gain unauthorised access to anyone else's computer or user account or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to any member of staff or contact the Head of ICT.

7 You must not attempt to access information about others or share information about others without their permission. To do so may breach data protection legislation and laws relating to confidentiality.

8 The school has security hardware and software meeting digital and technology standards in place to ensure the safety and security of the school's networks. You must not attempt to disable, defeat or circumvent any of the school's security facilities. Any problems with the security hardware or software must be reported to a member of staff or the Head of ICT who will notify the Director of Finance and Operations.

9 The school has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter.

10 Viruses and malware can cause serious harm to the security of the school's network and that of others. Viruses and malware are often spread through internet downloads or circulated as attachments to emails/electronic communications. If you think or suspect that an attachment, or other downloadable material, might contain a virus or malware, you must speak to a member of the IT team before opening the attachment or downloading the material.

11 You must not disable or uninstall any anti-virus, anti-malware or pupil-monitoring software on the school's computers including any school-owned devices issued to pupils for remote learning.

12 The use of location services can represent a risk to the personal safety of pupils and to school security. The use of any website or application, ~~whether on a school or personal device~~, with the capability of identifying the user's location while you are on school premises or otherwise in the care of the school is discouraged.

Appendix Two: Use of the internet and email/electronic communication services

1 The school does not undertake to provide continuous internet access. Email/ electronic communication services and website addresses at the school may change from time to time.

Use of the internet

2 You must use the school's computer system for educational purposes only and are not permitted to access interactive or networking websites during the school day unless you have express, prior consent of a member of staff.

3 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

4 You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not breach copyright or plagiarise (pass off as your own) another's work.

5 You must not load material from any external storage device brought in from outside the school onto the school's systems, unless this has been authorised by the Head of ICT.

6 You must not view, retrieve, download or share any illegal, offensive, potentially harmful or inappropriate material. Such material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, misogynistic/misandrist, homophobic, biphobic, pornographic, defamatory or that relates to any form of bullying or sexual violence/sexual harassment or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

7 You must not communicate with staff using social networking sites or other internet or web- based communication channels unless this is expressly permitted for educational reasons.

8 You must not bring the school into disrepute through your use of the internet.

Use of email/electronic communication services

9 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail or electronic communication devices, apps or platforms through the school's network without the express, prior consent of a member of staff.

10 Your school email/electronic communication accounts can be accessed using personal devices as well as with school-provided devices.

11 You must use your school email/electronic communication accounts e.g. the chat functionality of Microsoft Teams, any virtual learning environment, homework submission tool etc as the only mean(s) of electronic communication with staff. Communication either from a personal email account or to a member of staff's personal email/electronic communication account is not permitted.

12 Email/electronic communications should be treated in the same way as any other forms of written communication. You should not include or ask to receive anything in a message

which is not appropriate to be published generally or which you believe the school and / or your parents would consider to be inappropriate. Remember that messages could be forwarded to or seen by someone you did not intend.

13 You must not send or search for any messages which contain illegal, offensive, potentially harmful or inappropriate material. Such material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, misogynistic/misandrist, homophobic, biphobic, pornographic, indecent, defamatory or that relates to any form of bullying or sexual violence/sexual harassment or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material you must inform a member of staff as soon as possible. Use of the email/electronic messaging system in this way is a serious breach of discipline and may constitute a criminal offence.

14 Trivial messages and jokes should not be sent or forwarded through the school's email/electronic communication system. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the school's network to suffer delays and / or damage.

15 You must not use the school's email / electronic communication systems to send misogynistic messages or messages which contain language relating to sexual violence or which could be interpreted as being harassment, whether of a sexual nature or otherwise. The school has adopted a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The school will treat any such incidences as a breach of discipline and will deal with them under the school's Good Behaviour Policy and also as a safeguarding matter under the **school's** Safeguarding and Child Protection Policy and procedures.

16 Any correspondence from your school email/electronic communication account must contain the school's disclaimer.

17 You must not read anyone else's messages without their consent.

Other online communication by pupils (including social media, Zoom (chats) and Microsoft Teams)

18 Anything you post online whether through messaging, social media or by other means needs to be considered carefully. Remember that there is a 'disinhibition effect' making you more likely to post things you might regret. The **school may become involved in** anything between members of the school community or that may bring the school into disrepute. Private conversations are rarely private and should not be considered so.

19 Only post messages or images you would be happy for a teacher, parent or guardian to see. Avoid making strongly opinionated comments which could be deemed offensive. Avoid making comments related to protected characteristics.

20 Anonymous posting is unwise. If pupils set up accounts to post anonymously (or the presence of a group allows anonymity) all members of the group will be deemed individually responsible for material posted unless an individual admits responsibility. Nevertheless, other members of the group will be deemed partially responsible unless they have reported inappropriate posts or actively attempted to dissuade the perpetrator.

21 Do not make comments about individuals in the school community or about the school online. They may be your views, but they could cause offence and the internet is not the place for such comments.

22 Never pretend to be anyone else or any institution.

23 Do not harass others or post things intended to upset them. Do not troll.

24 Some messages and images may seem to be temporary and permanently deleted – this may not be the case if screenshots or photos are taken. Treat all **posts as permanent.**

25 Be cautious of meeting someone you meet online in real life. Always take an adult with you and tell people where you are going and who you are meeting.

26 Remember: once you share something it can be freely and easily copied, shared or manipulated. Once you've shared it – you've lost control of it.

27 Don't use tech in your bedroom as it affects sleep and can make it more likely that you will post something you will regret. It is also best to avoid using tech when tired. Switch off at least an hour before bedtime and leave devices out of the bedroom.

28 Consider how much tech you use in a day. Use of the internet and gaming can both be addictive and it is difficult to self-regulate use.

29 Be careful not to believe all you read online. Some sites publish dangerously inaccurate material. Be especially careful when investigating health concerns, sexuality and identity and searching for supportive communities.

30 Bring any concerns about your own use, or other people's, of tech, to the attention of a member of staff, promptly.

Appendix Three: Mobile Phones and Devices Policy

Context: While we recognise the benefits that come from a digitally connected world, at St Paul's Cathedral School we are committed to ensuring that our students have a distraction free learning environment, with their focus on their learning and on building strong, positive, face-to-face relationships with those present around them. We recognise that there are sensible uses for mobile phones in our community, for example when pupils are travelling independently to school.

Scope: this policy applies throughout our school, including EYFS and Boarding. (Note additional guidelines for boarders' use of electronic devices below and see also the additional policy: EYFS Policy for the Use of Cameras, Mobile Phones and Electronic Devices, included here as Appendix Four).

Our mobile phone rules: Mobile phones (and any devices with internet connectivity or capability, or recording capability, including smart watches) are not to be used by pupils during our school day or during any pre- or post-school activities.

We see this as an important way of actively promoting our pupils' wellbeing. We consider the unmediated pressures of social media and access to constant, instantaneous communication with peers inside and outside the school, and regular disruptions to learning, focus and social interaction in person, to be negative influences on our students and not a constructive part of their school day.

Travel: Pupils who travel alone to or from school, and whose parents decide that they wish them to have a phone with them for travel, may bring their phone on school premises. Parents are responsible for ensuring their child's phone is charged: charging facilities are not available during the school day except in an emergency. Phones must either be left in the basket at the front door on entry or handed to a member of the school Office team, who will place them in the basket. The phone must be switched off.

Sanctions: Failing to hand in a phone or internet-enabled device is a breach of our school rules and will be met with a sanction (ranging from one negative house point to a detention) at the discretion of the Deputy Head. Bringing in a second phone is regarded as a serious breach of school rules, and repeated use of a second phone could result in temporary exclusion (suspension).

Exceptions: There will be exceptions made to this policy, at the discretion of the Deputy Head or Head. Examples could include:

- a pupil who needs to monitor blood sugar levels and uses a phone app to do so, may be allowed supervised access to their phone as needed
- a pupil who requires access to their phone to report an e-safety issue to staff
- a pupil who requires access to a mental health app may be allowed to keep a phone with them as needed
- a disabled pupil requires access to their phone as a reasonable adjustment agreed with the school, consistent with the school's duties under the 2010 Equality Act
- a boarding pupil who needs to make contact with parents who are on a different time zone

All such arrangements will be discussed with parents in advance and will be recorded and monitored by the Deputy Head. In these circumstances, at the Deputy Head's discretion, parents may be requested to confirm that 4G or 5G connectivity, and/or particular apps or functions, are blocked on the phone.

School trips: On school trips, the trip leader, in consultation with the Deputy Head, will make and communicate a decision about whether pupils are allowed to bring mobile phones and internet-enabled devices. Priority will be given to ensuring that the educational and social experience of the pupils is not compromised by the presence of mobile phones. Pupils will be reminded that their acceptable use of IT agreement applies on the school trip.

The role of parents: Parents are expected to read and understand our mobile phones and devices policy and to discuss this with their children, bringing any concerns they may have regarding mobile phone usage promptly to their child's form teacher or to the Deputy Head.

The role of staff: Staff should consistently apply the school's policy on mobile phones, reporting any concerns to the Deputy Head.

Staff use of mobile phones: Staff should not use their personal mobile phones for personal reasons in front of pupils. They may need to use a phone for professional reasons, e.g. to set homework, to access our Management Information System (iSAMS) or to use MFA (multi-factor authentication). They may use their phones for security purposes when on duty outside in our playground. Trip phones are used on school trips and outings. Particular rules apply to the use of phones in EYFS: please see the EYFS Policy for the Use of Cameras, Mobile Phones and Electronic Devices.

Rules for Boarders regarding electronic devices in Boarding Time
All rules above apply to Boarders during the school day. The following extract from the Boarding Handbook sets out rules for devices in boarding time, and applies also to smart watches and any internet/recording capable device.

.

Electrical equipment such as mobile phones, video and audio devices and pocket games may be brought in from home and used in school at set times as detailed in the boarders' Weekly Schedule with the permission of the Head of Boarding. This is under careful supervision of the Boarding staff. At all other times devices should be locked away in the cupboard situated in the dining room. Chargers for such devices will be tested annually along with all other portable appliances, as specified in the Health and Safety framework. An up-to-date register of all electronic devices and phones is kept, which provides a record of what the boarders have access to in school.

.

Deputy Head Spring Term 2024

Appendix Four: Photographs

Photographs and images

1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute serious misbehaviour.

2 You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.

3 If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted: the device will be delivered to the police, as stated in paragraph 12.3 of this policy.

4 If material found on a device is a still or moving image that has been obtained by 'upskirting' this will not be deleted: the device will be delivered to the police, as stated in paragraph 12.3 of this policy.

5 You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. Staff will not view or forward illegal images of children.

6 The posting of images considered to be offensive or which brings the school into disrepute, is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using school or personal facilities.

7 Sharing nude and semi-nude images and videos

7.1 "Sharing nudes and semi-nudes" means the consensual (with permission) and non-consensual (without permission) taking and sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. This could be via social media, gaming platforms, chat apps or forums. It can also involve sharing between devices offline e.g. via Apple's AirDrop. This may also be referred to as ‘sexting’ or youth produced sexual imagery.

7.2 Sharing or soliciting sexual images is strictly prohibited, whether or not you are in the care of the school at the time the image is recorded and / or shared. This includes the sharing of digitally manipulated or AI-generated materials.

7.3 Sexting may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image. Even if you are not prosecuted, this may result in information being stored on your police record, which may prevent you from obtaining certain jobs in the future and may impact your freedom of travel.

7.4 The police may seize any devices which they believe may have been used for sexting. If the police find that a device contains inappropriate images, they are unlikely to return it to you.

7.5 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied, and may be shared by others.

7.6 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

7.7 Even if you don't share images yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

7.8 The school will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the school's child protection procedures (see the school's *Safeguarding and Child Protection Policy*).

7.9 If sexual images or videos have been made and circulated online, you can be supported to get the images removed through the Internet Watch Foundation.

7.10 If you are concerned about any image you have received, sent or forwarded, or otherwise seen, speak to any member of staff for advice.

8 Upskirting

8.1 Upskirting typically involves taking a picture under a person's clothing without their permission and/or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm.

8.2 Upskirting is strictly prohibited, whether or not you are in the care of the school at the time the image is recorded.

8.3 Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.

8.4 The school will treat incidences of upskirting as a breach of discipline and also as a safeguarding matter under the school's child protection procedures (see the school's Safeguarding and Child Protection Policy).

8.5 If you are concerned that you have been a victim of upskirting, speak to any member of staff for advice.

Appendix Five: Online Sexual Harassment

1 Online sexual harassment means "unwanted conduct of a sexual nature" occurring online, whether in school or outside of it.

2 The school takes a zero tolerance approach to online sexual harassment: it is never acceptable and it will not be tolerated. The school will treat incidences as a breach of discipline and will deal with them under the school's Good Behaviour Policy and also as a safeguarding matter under the school's child protection procedures (see the school's Safeguarding and Child Protection Policy and procedures).

3 All allegations will be responded to seriously and all victims will be reassured and offered appropriate support, regardless of how long it has taken for them to come forward, and kept safe.

4 The school will consider online sexual harassment in broad terms, recognising that it can occur between two or more children of any age or sex and through a group of children sexually harassing a single child or group of children.

5 It will consider whether incidents of online sexual harassment are standalone, or part of a wider pattern of sexual harassment and / or sexual violence. It may include:

5.1 consensual and non-consensual sharing of nude and semi-nude images and/or videos;
5.2 sexualised online bullying;
5.3 unwanted sexual comments and messages, including on social media;
5.4 sexual exploitation, coercion or threats; and
5.5 coercing others into sharing images of themselves or performing acts they're not comfortable with online.

6 If a pupil is concerned that they have been a victim of online sexual harassment, they must speak to any member of staff for advice.

7 When dealing with online sexual harassment staff will follow the school's Safeguarding and Child Protection Policy and procedures.

8 The Head and staff authorised by the Head have a statutory power to search pupils / property on school premises. This includes content of mobile phones and other devices, if there is reasonable suspicion that a device contains illegal or undesirable material relating to online sexual harassment. The school's search procedures can be found in the school's Good Behaviour Policy.

Appendix Six:

Harmful online challenges and online hoaxes

1 A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge or following a trend, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

2 The school takes a proactive approach to negative online behaviours, teaching about them in ICT lessons, PSHE and through assemblies on online safety.

3 If the school becomes aware that harmful online challenges or online hoaxes are circulating between pupils, the school will handle this as a safeguarding matter under the school's child protection procedures (see the school's Safeguarding and Child Protection Policy and procedures).

4 The DSL (Deputy Head, Mrs Heylen) will take a lead role in assessing the risk to the school community, undertake a case by-case assessment, including considering if the risk is a national one or localised to the area, or just the school. Parents may be alerted, depending on the nature of the hoax/harmful online challenge.

5 The factual basis of any harmful online challenge or online hoax will be checked through known reliable and trustworthy sources e.g. the Professional Online Safety Helpline, Childnet, local safeguarding partners or City of London police force.

6 If, following investigation, the DSL finds that pupils have deliberately shared information with the intention of encouraging others to participate in harmful online challenges or online hoaxes, this will be treated as a breach of discipline and will be dealt with under the school's Good Behaviour Policy.

7 The Head and staff authorised by the Head have a statutory power to search pupils / property on school premises. This includes content of mobile phones and other devices if there is reasonable suspicion that a device is being used to commit an offence or cause personal injury or damage to property. The school's search procedures can be found in the Good Behaviour Policy.

Appendix Seven:

Acceptable Use Agreements

St Paul's Cathedral School
ICT Acceptable Use Agreement for Pupils

This agreement applies to all sections of the school, including Boarders and Early Years. Pre-prep parents read this agreement on their child's behalf. There is a simplified form for Pre-prep in Section 2.
These rules apply at school and also outside of school, when using school-provided equipment or systems (e.g. if you are using a school iPad or Google Classroom or your school email address).

Why do we have an Acceptable Use Agreement?

Kindness is our cornerstone at SPCS. Respect for yourself and for one another is at the heart of our community. We want you to use the amazing learning and entertainment opportunities of the internet, while staying safe and making sure others are safe too.

Section 1 (Read this carefully before signing if you are in Years 3-8)

Using the Network

I will only log on to the system using the username and password given to me by the school.
I will respect other people's work and not interfere with another person's files in their directory.
I will not connect USB sticks (pen drives) or other portable data storage devices to the network in any way.
I will not do anything to cause damage to the computers or change, damage or try to damage the data stored on them in a way that causes harm.
I will be responsible for making sure my account is logged off at the end of each session and that I return any IT equipment I have been given.
I will follow the school rules about mobile phones:

Day Pupils: leaving them in the basket in Reception until allowed to collect them at the end of the school day
Boarding Pupils: leaving them with Boarding staff and using only when permitted

Using electronic communications

- Whenever I am online at school **or away from school** I will not annoy, upset or harass other members of the school community with offensive, obscene (very rude), abusive, or threatening language in any electronic communication.
- **I understand that this behaviour is cyberbullying and SPCS has zero tolerance for bullying of any kind.**
- **I know that cyberbullying will be treated as serious misbehaviour which could risk my place at the school.**
- **If I become aware that another member of the community is being cyberbullied, I will report this to a trusted adult at home or school.**
- I will not give any contact details (address, phone number) or make arrangements to meet an unknown person using any electronic communication.

- If I receive any electronic communication that I do not like, I will tell a trusted person straight away.
- I know that opening attachments can damage the system. I will seek permission to open any electronic attachment if I am unsure of its content.

Using the Internet

- I will show respect when choosing the sites I visit and will not deliberately try to access any Internet sites that I think a parent or teacher would reasonably consider inappropriate in a school environment.
- I will not download games, music, images or video from the Internet that are subject to copyright (that belong to other people). If I am not sure, I will check with a teacher.
- I understand that I must respect other people's copyright. I will not download text written by someone else to use as my own.
- I will not try to sell or buy anything on the Internet whilst at school.
- If I access anything that I am unhappy with I will tell a trusted person straight away.
- Social media and networking sites such as X (formerly Twitter), Instagram, TikTok and Facebook are blocked by the school filter. Pupils are reminded that social networks carry age restrictions and that they must not own an account on any social network under the age of 13.
- I will not post, 'like' or forward any comments, photographs or videos to these sites, YouTube, or similar sites which would be derogatory (rude about or negative) to the school or the school community, or threaten, insult, or bully members of staff or other pupils.
  I understand that doing this will be seen as serious misbehaviour (cyberbullying) and may result in disciplinary action being taken by the school.

Monitoring

- Filtering is a process which cuts down the risk of us accessing something unsuitable for us on the Internet.
- I understand that the school operates filtering to keep all users safe from harmful content and that the web sites I visit are checked by the school.
- I understand the school may check my files, the electronic communications I send and receive and the web sites I visit.
- I understand that if I deliberately break these rules it will be seen as serious misbehaviour, may mean that I am banned from using school IT and may even risk my place in the school community.
- I understand the school can check the use of the network facilities by looking at my search history, emails and files, and delete inappropriate material, to make sure that the rules above are being followed.

I agree to follow the rules above.

I understand that these rules have been designed to create a safe environment for me and others to access the Internet and use computers for learning.
If I think that I have broken any of these rules, accidentally or on purpose, or become aware that someone else has done so, I will report this straight away to an adult at home or school.

Name of pupil: ----------
Pupil signature: ---------- Date: ----------

Section 2 (FOR PRE-PREP)

Acceptable use of ICT: Golden Rules for Pre-Prep

Please read the Golden Rules for Pre-Prep below and share with your child. Then fill in the details at the bottom of the page to give your agreement.

Why do we have ICT Golden Rules?

To keep you and everybody else in our community as safe as possible when you are learning on school computers and tablets.

Use of equipment:

- I will only use school computers and tablets when I have been given permission by an adult.
- I will be careful when using school ICT equipment to avoid any damage.
- I will respect others' work and will not delete it.
- I will not take photos or videos on the iPads without permission.
- I will show **respect and kindness** when I use school ICT equipment.

Responsible Internet Use:

- I will only use the internet and email when I have permission from an adult.
- I will ask an adult when I am unsure what to click on so that I don't see or download something by mistake.
- I will not share any information about myself or others on the internet.
- I will not talk or write to other people online without permission.
- If I see something I don't like on a screen, I will always show an adult straight away.
- If I am unsure of any question that 'pops up', I will ask permission from an adult before I click an answer.
- I will show **respect and kindness** when I use the internet.
- **If I have any worries** when I am using ICT equipment, **I will tell an adult**.

Parents: please complete this section to show that your child has understood and agreed to the rules. Contact the Head of Pre-prep, Miss Smyth, with any questions.

We have discussed these guidelines and my child has agreed to follow these rules.

Name of pupil:
Name of parent:
Parent signature