ST PAUL'S CATHEDRAL SCHOOL

Online Safety Policy

Academic Year 2025-2026

Review: September 26

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 Online Safety Policy of St Paul's Cathedral School (**the school**).

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which empowers the school to:

1.2.1 protect the whole school community from illegal, inappropriate and harmful content or contact;

1.2.2 educate the whole school community about their access to and use of technology;

1.2.3 establish effective mechanisms to identify, intervene in and escalate concerns where appropriate; and

1.2.4 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 at the school and seeks to ensure that the best interests of pupils underpins and is at the forefront of all decisions, systems, processes and policies.

1.4 Online safety is a running and interrelated theme throughout many of the school's policies and procedures (including its Safeguarding and Child Protection Policy and Procedures) and careful consideration has been given to ensure that it is also reflected in the school's curriculum, teacher training and parental engagement, as well as the role and responsibility of the school's Designated Safeguarding Lead and any deputies.

1.5 The school seeks to ensure that our safeguarding related policies and procedures are transparent, clear and easy to understand for staff, pupils, parents and carers. The school welcomes feedback on how we can continue to improve our policies and practices.

2 **Scope and application**

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

2.2 This policy applies to all members of the school community, including staff and volunteers, pupils, parents and visitors, who have access to the school's technology whether on or off school premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the school community or where the culture or reputation of the school is put at risk.

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 Early years foundation stage statutory framework for group and school-based providers (DfE, September 2025);

3.1.3 Education and Skills Act 2008;

3.1.4 Children Act 1989

3.1.5 Childcare Act 2006;

3.1.6 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR);

3.1.7 Equality Act 2010; and

3.1.8 National minimum standards for boarding schools (DfE, September 2022).

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2025) (KCSIE);

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 Science, Innovation & Technology (DSIT) and UK Council for Internet Safety (UKCIS), March 2024);

3.2.4 Prevent duty guidance: for England and Wales (Home Office, October 2023, in force on 31 December 2023);

3.2.5 Channel duty guidance: protecting people susceptible to radicalisation (Home Office, October 2023, updated December 2023).

3.2.6 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, September 2021);

3.2.7 Searching, screening and confiscation: advice for headteachers, school staff and governing bodies (DfE, July 2022, in force from September 2022);

3.2.8 Safeguarding children and protecting professionals in early years settings; online safety considerations (UKCIS, February 2019);

3.2.9 Behaviour in schools: advice for headteachers and school staff 2022 (DfE, February 2024);

3.2.10 Mobile phones in schools 2024 (DfE, February 2024);

3.2.11 Teaching online safety in schools (DfE, January 2023);

3.2.12 Harmful online challenges and online hoaxes (DfE, February 2021);

3.2.13 Meeting digital and technology standards in education (DfE, maintained);

3.2.14 Appropriate filtering for education settings (UKSIC, May 2025);

3.2.15 Appropriate monitoring for schools (UKSIC, May 2025);

3.2.16 Generative AI: product safety expectations (DfE, January 2025);

3.2.17 Plan technology for your school (HM Government, September 2024)

3.3 The following school policies, procedures and resource materials are relevant to this policy:

3.3.1 Acceptable Use of ICT Policy for Pupils;

3.3.2 Acceptable Use of ICT Policy for Staff

3.3.3 Safeguarding and Child Protection Policy;

3.3.4 Anti-Bullying Policy;

3.3.5 Good Behaviour Policy;

3.3.6 School Rules

3.3.7 Staff Code of Conduct and Whistleblowing Policy;

3.3.8 Data Protection Policy;

3.3.9 Relationships Education and Relationships and Sex Education policy;

3.3.10 Privacy Notice

4 **Publication and availability**

4.1 This policy is published on the school website.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from the school office during the school day.

4.4 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 **Designated Safeguarding Lead** (DSL) are references to the Deputy Head who is the DSL.

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

5.1.2 In considering the scope of the school's online safety strategy, the school will take a wide 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**).

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 and for approving and reviewing its effectiveness.

6.2 The Board of Governors is required to ensure that all those with leadership and management responsibilities at the school actively promote the well-being of pupils. The adoption of this policy is part of their response to this duty.

6.3 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)	Annually
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	Head of IT/ Deputy Head	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/Head of IT	Annually
Formal Annual Review	DSL	Annually

7 Role of Staff **and parents**

7.1 **Head and Senior Leadership Team**

7.1.1 The Head has overall executive responsibility for the safety and welfare of members of the school community. This includes a specific responsibility to ensure that the school has an effective filtering policy in place and that it is applied and updated on a regular basis.

7.1.2 The Designated Safeguarding Lead is the senior member of staff from the school's leadership team with lead responsibility for safeguarding and child protection, including online safety and understanding and overseeing the filtering and monitoring systems in place in school.

(a) The responsibility of the Designated Safeguarding Lead includes;

(i) managing safeguarding incidents involving the use of technology (including through the use of generative AI) in the same way as other safeguarding matters, in accordance with the school's Safeguarding and Child Protection Policy;

(ii) Working with the Head of ICT and IT Manager to ensure all staff are appropriately trained and aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents;

(iii) Working with the IT Manager and Head of ICT in monitoring technology uses and practices across the school and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

(iv) Overseeing and acting on filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems;

(v) Regularly working with the IT Manager and Head of ICT to assess whether changes need to be made to policies and staff and pupil training;

(vi) Regularly updating other members of the school's Senior Leadership Team and the Governors on the operation of the school's safeguarding arrangements, including online safety practices;

(vii) Providing online safety training and advice to governors, staff, parents, carers and pupils including on online harms and how to identify illegal, harmful or inappropriate content created or accessed through the use of generative AI; and

(viii) Promoting an awareness of and commitment to online safety education / awareness raising across the school and beyond.

7.2 **Head of ICT**

7.2.1 The Head of ICT is a member of the staff team with lead responsibility for digital technology. They act as a link between technical staff, the SLT, curriculum leads, data protection lead (Director of Finance and Operations), the DSL.

7.2.2 The Director of Finance and Operations, IT Manager and the Head of IT work jointly on development of IT infrastructure and developing user experience, led by the needs of staff and students.

7.2.3 The Deputy Head Academic, in consultation with the Head of IT and Director of Finance and Operations, will be accountable and responsible for:

(a) developing digital strategy based on teaching and learning outcomes and organisational needs;

(b) encouraging and supporting the use of digital technology (including through the use of generative AI) across the school;

(c) identifying and acting on digital technology training needs for staff and students;

(d) reviewing registers relating to hardware and systems to ensure they are up to date;

(e) reviewing measures in place on the school's use of generative AI and measures taken to combat cybercrime;

(f) proactively identify any potential compromises to safeguarding or risk of a cyber-attach to ensure compliance with the Cyber security standards; and

(g) ensuring digital technology is included within insurance arrangements and disaster recovery and business continuity plans.

7.3 **IT Manager**

7.3.1 The IT Manager, under the oversight of the DSL, is responsible for the effective operation of the school's filtering and monitoring systems so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the school's network.

7.3.2 The IT Manager is responsible for ensuring that:

(a) the school's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the school's technology if they are properly authenticated and authorised;

(c) the school's filtering and monitoring systems are maintained, filtering and monitoring reports are provided and actions following concerns or checks to systems are completed;

(d) the risks of pupils and staff circumventing the safeguards put in place by the school are minimised;

(e) the use of the school's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the IT team to monitor the use of email and the internet over the school's network and maintain logs of such usage.

(g) reviewing the effectiveness of IT support to inform decision making and taking action, when necessary;

(h) identify any potential compromises to safeguarding or risk of a cyber-attack;

(i) ensuring digital technology is considered appropriately for disaster recovery and business continuity planning purposes.

7.3.3 Summary of filtering arrangements:

(a) Using a software application Sophos Firewall and Fastvue Alerts, the school monitors all essential hardware and software services. Email alerts are sent to the IT Manager 24/7 alerting them of problems and potential problems on the network.

(b) The IT Manager reports to the Director of Finance and Operations, DSL and Head of ICT regularly

(c) The IT Manager receives instant emails from Fastvue listing users who have visited inappropriate sites or tried to download inappropriate content. The IT Manager will escalate concerns to the DSL as necessary.

7.3.4 The IT Manager reports regularly to the Director of Finance and Operations on the operation of the school's technology. If the Head of ICT has concerns about the functionality, effectiveness, suitability or use of technology within the school, including the monitoring and filtering systems in place, they will escalate those concerns promptly to the Designated Safeguarding Lead or Director of Finance and Operations as appropriate.

7.4 **All staff**

7.4.1 All staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.4.2 Training of all staff includes online safety which, amongst other things, includes an understanding of filtering and monitoring provisions in place, how to manage them effectively, the use of generative AI and the risks associated with this, how to escalate concerns when identified and any particular expectations or responsibilities in relation to filtering and monitoring.

7.4.3 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the school's policies and of safe practice with the pupils.

7.4.4 Staff should follow the guidance covering the use of technology in the classroom which is contained in the *Acceptable Use of IT Policy for Staff*.

7.4.5 All staff are aware that technology (including the use of generative AI) can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

7.4.6 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery This includes the sharing of digitally manipulated or AI-generated images;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content; and/or

(d) cyberbullying,

7.4.7 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and/or encourages physical abuse;

(b) facilitates, threatens and/or encourages sexual violence; or

(c) is used as part of initiation/hazing type violence and rituals.

7.4.8 It is important that staff recognise the indicators and signs of child on child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child on child abuse at the school, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

7.4.9 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" or "girls being girls" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse. The school has a **zero tolerance approach** towards child on child abuse (including in relation 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.

7.4.10 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the school's Safeguarding and Child Protection Policy. If staff have any concerns regarding child on child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the Designated Safeguarding Lead in all cases.**

7.5 **Parents**

7.5.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The school expects parents to promote safe practice when using technology and to:

(a) support the school in the implementation of this policy and report any concerns in line with the school's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour;

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support; and

(d) support the school's policy on prohibiting the use of mobile phones.

7.5.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead. They can also consult the online safety resources detailed in this policy.

8 **Filtering and monitoring**

8.1 In respect of their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, the Governors will do all they reasonably can to limit pupils' exposure to risks from the school's IT system. As part of this process, the school has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness.

8.2 The school has regard to Government filtering and monitoring standards, which require that the school;

8.2.1 Identifies and assigns roles and responsibilities to manage filtering and monitoring systems;
8.2.2. Reviews filtering and monitoring provision at least annually;
8.2.3 Blocks harmful and inappropriate content without unreasonably impacting teaching and learning; and
8.2.4 Has effective monitoring strategies in place that meet their safeguarding needs.

8.3 The school will assess its approach to filtering and monitoring to reflect the risks it faces and will continue to assess this in light of new or emerging risks and technologies.

8.4 The school manages access to content across its systems for all users, including guest access. Logs / alerts are regularly reviewed and acted upon.

8.5 The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc).

8.6 The school understands the extent to which content is dynamically analysed where it is streamed in real-time (including content created by users or through generative AI) to the user and blocked.

8.7 Access to content through non-browser services eg apps and other mobile technologies is managed in ways that are consistent with this policy.

8.8 The school has monitoring systems in place to protect the school, systems and users. It monitors all network use across all its devices and services. Logs/alerts are regularly reviewed and acted upon.

8. The school uses a number of monitoring strategies to minimise safeguarding risks on internet connected devices, including;

8.9.1 Physical monitoring by staff watching screens of users;

8.9.2 Live supervision by staff on a console with device management software within the ICT suite;

8.9.3 Network monitoring using log files of internet traffic and web access; and

8.9.4 Individual device monitoring through software or third-party services.

9 **Access to the school's technology**

9.1 The school provides internet, intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective Acceptable Use of ICT Policy when using school technology. All such use is monitored by the IT department.

9.2 Pupils and staff require individual user names and passwords to access the school's internet, intranet and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their user names or passwords must report it to the IT department immediately.

9.3 The use of any personal device connected to the school's network will be logged and monitored by the IT Manager. Pupils do not have access on personal device via the school Wi-Fi. Appropriate

use of the school's network is covered within the acceptable use of ICT policy for pupils. When connecting devices to the school's WiFi, staff sign in using their school credentials. There is a single login for guests which is monitored in the same way as a staff account. See also 9.4 below and the school's information security and sharing data guidance for staff (including remote working and bringing your own device to work).

9.4 **Inappropriate material**

9.4.1 The school recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

9.4.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead.

The term 'online safety' encapsulates a wide range of issues but these can be classified into four main areas of risk:

(a) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories);

(b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);

(c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

(d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If pupils or staff are at risk, it should be reported to the Anti-Phishing Working Group

9.5 **Use of mobile electronic devices and smart technology**

9.5.1 The school has adopted a policy that prohibits pupils in the school to use personal mobile electronic devices.

9.5.2 The school rules about the use of mobile electronic devices or other smart technology, including access to open/non-school networks and the use of generative AI tools, are set out in the *Acceptable Use of ICT Policy for Pupils*.

9.5.3 The school will consider whether adaptations and reasonable adjustments to this policy need to be made for individual pupils e.g. to manage medical conditions or for safeguarding reasons. These will be considered on a case-by-case basis and permission to do so must be sought and given in advance. These cases will be communicated in advance with all academic and related support staff.

9.5.4 The school does all that it reasonably can to limit children's exposure to the risk identified above through the use of the school's IT system.

9.5.5 The school has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email, and social media sites) on school devices that are connected to the school's network and their effectiveness is regularly reviewed.

9.5.6 Mobile devices and smart technology equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. The school is alert to the risks that such access presents, including the risk of pupils sexually harassing, bullying or controlling their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually (often via large group chats); or viewing and/or sharing pornography and other harmful content (including content created by generative AI tools in real-time). The school has adopted the approach to mobile electronic devices as stated in The school's *Acceptable use of ICT Policy for pupils* as a mechanism to manage such risks.

9.5.7 (a) Day pupils are not permitted to use their phones or other devices with connectivity capability in school.

(b) Day pupils must leave phones and other mobile devices with reception during the school day; and

(c) Boarders have 'brick' (non-smart) phones and these are left in the supervision of residential staff other than when they are given to boarders for use of the devices during supervised windows.

9.5.8 The use of mobile electronic devices by staff is covered in the Staff Code of Conduct, Acceptable Use of ICT Policy for Staff, (including remote working and bringing your own device to work).

9.5.9 The school's policies apply to the use of technology by staff and pupils whether on or off school premises and appropriate action will be taken where such use affects or could affect the welfare of other pupils or any member of the school community or where the culture or reputation of the school is put at risk.

10 **Procedures for dealing with incidents of misuse**

10.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the school in accordance with this policy and the school's safeguarding and disciplinary policies and procedures.

10.2 The school recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to shared further (e.g. with the Designated Safeguarding Lead) to discuss next steps. Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those who are victims of abuse, children with SEN or disabilities.

10.3 **Misuse by pupils**

10.3.1 Anyone who has any concern about the misuse of technology by pupils should report

it immediately so that it can be dealt with in accordance with the school's behaviour

and discipline policies, including the *Anti-Bullying Policy* where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-bullying	Form Tutor / teacher or trusted member of staff.
Sexual violence and sexual harassment (whether during or outside of school)	Safeguarding and Child Protection Policy	The DSL, who has overall responsibility for online safety matters
Sharing nudes and semi-nude images (sexting / youth produced sexual imagery) including creation or sharing of adapted or 'deep fake' images.	Safeguarding and Child Protection Policy	Form Tutor / teacher or trusted member of staff. Who should then refer to the DSL who has overall responsibility for safeguarding including online safety matters
Harassment	Safeguarding and Child Protection Policy	
Upskirting	Safeguarding and Child Protection Policy	
Radicalisation	Safeguarding and Child Protection Policy	
Other breach of acceptable use policy, including unauthorised use of mobile devices during teaching hours.	See relevant policy referred to in acceptable use policy	Form Tutor / teacher or trusted member of staff. Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead

Any action resulting in disruption to digital technology systems in school should be reported to the IT Manager or Director of Finance and Operations, or in their absence to any member of the Senior Leadership Team.

10.3.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the school's child protection procedures (see the school's *Safeguarding and Child Protection Policy*).

10.4 **Misuse by staff**

10.4.1 Anyone who has any concern about the misuse of technology by staff should report it in accordance with the school's *Whistleblowing Policy* so that it can be dealt with in accordance with the staff disciplinary procedures.

10.4.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they must report it immediately in accordance with the school's policy on raising concerns and dealing with allegations which is set out in the school's *Safeguarding and Child Protection Policy*.

10.4.3 Anyone who has any other concern about the misuse of technology by staff should report their concerns as set out below:

(a) Staff should speak to the DSL (if safeguarding-related) or Director of Finance and Operations (if network or systems-related) or in their absence to any member of the Leadership Team in accordance with the school's *Whistleblowing Policy*; and

(b) Anyone else should speak to the Head.

(c) If the report relates to the Head, it can be brought to the DSL or Chair of Governors

10.5 **Misuse by any user**

10.5.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the Director of ICT, the Designated Safeguarding Lead, the Director of Finance and Operations or the Head.

10.5.2 The school reserves the right to withdraw access to the school's network by any user at any time and to report suspected illegal activity to the police.

10.5.3 If the school considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

11 **Education**

11.1 The teaching of online safety is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning.

11.2 The school ensures that children are taught how to keep themselves and others safe, including online, and the safe use of technology is therefore integral to the school's curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices and on the use of generative AI tools. Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those who are victims of abuse, children with SEN or disabilities.

11.3 Technology is included in the educational programmes followed in the EYFS in the following ways:

11.3.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

11.3.2 children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

11.3.3 children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

11.4 The safe use of technology is also a focus in all areas of the curriculum teacher training and key safety messages are reinforced as part of assemblies, PSHE and tutorial / pastoral activities, teaching pupils:

11.4.1 about the risks associated with using the technology (including through generative AI) and how to protect themselves and their peers from potential risks;

11.4.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "banter" or "just boys being boys" or "girls being girls"

11.4.3 to be critically aware of content they access online and guided to validate accuracy of information;

11.4.4 how to recognise suspicious, bullying or extremist behaviour;

11.4.5 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

11.4.6 relevant laws applicable to the internet

11.4.7 the consequences of negative online behaviour;

11.4.8 Understanding the risks of bias or misleading information that can be produced by automated and AI generated content;

11.4.9 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the school will deal with those who behave badly; and

11.4.10 how to respond to harmful online challenges and hoaxes.

11.5 The school recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, misogyny/misandry, homophobia, biphobia and sexual violence and sexual harassment.

11.6 Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The school has 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.

11.7 The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

11.8 The school's *Acceptable Use of ICT Policy for Pupils* sets out the school rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

11.9 The school recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils. For more details on the school's approach, the school's *Safeguarding and Child Protection Policy* and its *Relationships Education and RSE Policy*.

11.10 **Useful online safety resources for pupils**
11.10.1 https://www.childnet.com/resources/smartie-the-penguin/
11.10.2 https://www.childnet.com/resources/digiduck-stories/
11.10.3 http://www.childnet.com/young-people
11.10.4 https://www.saferinternet.org.uk/advice-centre/young-people
11.10.5 https://mysafetynet.org.uk/
11.10.6 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/ 11.10.7 https://www.bbc.com/ownit

12 **Training**

12.1 **Proprietor**

12.1.1 To ensure that all Governors and Trustees are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of the school are effective and that they support the delivery of a robust whole school approach to safeguarding, all Governors and Trustees receive appropriate safeguarding and child protection (including online safety) training at induction. This training is regularly updated.

12.2 **Staff**

12.2.1 The school provides training on the safe use of technology to staff so that they 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.

12.2.2 Induction training for new staff includes training on the school's online safety approach, including this policy, the *Code of Conduct for Staff* and *Acceptable Use of ICT Policy for Staff*. 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 and radicalisation and dealing with harmful online challenges and hoaxes. This training may be in addition to the regular safeguarding and child protection (including online safety) training as required at induction and at least annually thereafter. Training specifically addresses the school's filtering and monitoring provisions in place, how to manage them effectively, how to escalate concerns when identified and any particular staff expectations or responsibilities, including on the use of approved generative AI tools for educational purposes.

12.2.3 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, dealing with harmful online challenges and online hoaxes and on the risks associated with generative AI tools and content created by them. This training may be in addition to the regular safeguarding and child protection (including online safety) updated as required at induction and at least annually thereafter.

12.2.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

12.2.5 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the school's policy on sharing nudes and semi-nude images and videos as set out in The school's Safeguarding and Child Protection Policy and Searching, screening and confiscation: advice for schools. In certain cases, it may be appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

12.2.6 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' where safeguarding is concerned, including in relation to sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and/or violent behaviour in the future

12.2.7 Staff are trained to recognise any illegal, inappropriate or harmful content, including content created generate through generative AI tools, and look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the school will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the school that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and/or staff training will be delivered to minimise the risk of it happening again.

12.2.8 Staff also receive data protection training on induction and at regular intervals afterwards.

12.2.9 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the school's overarching approach to safeguarding.

12.2.10 **Useful online safety resources for staff**

(a) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

(b) http://www.childnet.com/teachers-and-professionals

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online- safety/

(d) https://www.thinkuknow.co.uk/teachers/

(g) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)

(h) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

(i) Sharing nudes and semi-nudes: advice for education settings working with children and young people (DSITand UKCIS, March 2024)

(j) Online safety in schools and colleges: questions from the governing board (UKCIS, October 2022)

(m) Online Sexual Harassment: Understand, Prevent and Respond Guidance for schools (Childnet, March 2019)

(p) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, January 2023)

(q) Harmful online challenges and online hoaxes (DfE, February 2021)

(s) NSPCC helpline for anyone worried about a child - 0808 800 5000

(t) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

12.3 **Parents**

1. 12.3.1 The school is in regular contact with parents and carers and uses communications to reinforce the importance of ensuring that children are safe online. The school aims to help parents understand what systems are in place to filter and monitor their child's online use and ensures that parents are aware of what their children are being asked to do online (including what sites they will be asked to access) and who from the school they will be interacting with online, if anyone.
2. 12.3.2 The school works closely with parents to ensure they can safeguard their children whilst using technology. Information is regularly sent through the newsletter and via talks for parents. Parents are also advised upon best practice and introduced to current trends during tutorial evenings.
3. 12.3.3 Parents are encouraged to read the *Acceptable Use of ICT Policy for Pupils* with their child to ensure that it is fully understood.
4. 12.3.4 Parents have an important role in supporting the school's policy on prohibiting the use of mobile phones . Parents are encouraged to reinforce and discuss this policy with pupils, including the risks associated with mobile phone use and the benefits of a mobile phone free environment.
5. 12.3.5 Where parents need to contact their child during the school day, they should be directed to the school office, where staff should be aware of the school's policy on relaying messages and facilitating contact.

12.3.6 **Useful online safety resources for parents and staff**

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

(b) http://www.childnet.com/parents-and-carers

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online- safety/

(d) https://www.thinkuknow.co.uk/parents/

(e) https://www.thinkuknow.co.uk/parents/articles/theres-a-viral-scare-online-what-should-i-do/

(f) http://parentzone.org.uk/

(g) https://www.internetmatters.org/

(h) https://www.commonsensemedia.org/

(i) Advice for parents and carers on cyberbullying (DfE, November 2014)

(j) https://www.askaboutgames.com/

(k) https://www.ceop.police.uk/safety-centre

(l) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

(m) https://safeblog.lgfl.net/2018/11/parents-scare-or-prepare

13 **Cybercrime**

13.1 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).

13.2 Cyber-dependent crimes include;

13.2.1 unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

13.2.2 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

13.2.3 making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

13.3 The school is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

13.4 If staff have any concerns about a child in this area, they should refer the matter to the Designated Safeguarding Lead immediately. The Designated safeguarding Lead should 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. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. (Cyber Choices does not currently cover

'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.)

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 assessments 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.

14.3 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 Head has overall responsibility for ensuring that matters which affect pupil welfare 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 Designated Safeguarding Lead who may delegate (as appropriate) the assessment to staff who have been properly trained in, and tasked with, carrying out the particular assessment.

15 **Record keeping**

15.1 All records created in accordance with this policy are managed in accordance with the school's policies that apply to the retention and destruction of records.

15.2 All serious incidents involving the use of technology will be logged centrally in the IT incident log by the IT Manager and as part of the pupil or staff record.

15.3 The information created in connection with this policy may contain personal data. The school's use of 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 compliance is set out in the school's data protection policies and procedures when handling personal data created in connection with this policy. In addition, staff must ensure that they follow the school's data protection policies and procedures.

Review: September 26