Exeter School

Online safety policy

Status:	Approved
Approver:	SLG
Source (author):	ALM
Last review date:	September 2025
Next review date:	September 2026

Contents

1 Aims

1.1 This is the online safety policy of Exeter School (**School**), Department for Education number 878/6033, comprising:

1.1.1 the junior school for pupils in Year 3 to Year 6; and

1.1.2 the senior school for pupils in Year 7 to Year 13.

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 potentially 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 the devising and implementation of 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 any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead (**DSL**) (and any deputies).

1.5 Although this policy is necessarily detailed, it is important 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.

2 Scope and application

2.1 This policy applies to Exeter School. Please refer to the website for the separate policies for Exeter Pre-Prep School (Department for Education number 878/6046) including the Online safety policy of Exeter Pre-Prep School.

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 Education and Skills Act 2008;

3.1.3 Children Act 1989;

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

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

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

3.2.9 Relationships Education, Relationships and Sex Education (**RSE**) and Health Education guidance (DfE, 2021);

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

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

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

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

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

3.2.15 Online safety guidance if you own or manage an online platform (DSIT, June 2021);

3.2.16 A business guide for protecting children on your online platform (DSIT, June 2021);

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

3.2.18 Online safety audit tool (UKCIS, October 2022);

3.2.19 Appropriate Filtering for Education Settings (UKSIC, May 2025);

3.2.20 Appropriate monitoring for schools (UKSIC, May 2025); and

3.2.21 Online Safety Self-Review Tool for Schools, 360safe.

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

3.3.1 IT Acceptable usage policy (pupils);

3.3.2 Safeguarding and child protection policy and procedures;

3.3.3 Anti-bullying policy;

3.3.4 Risk assessment policy for pupil welfare;

3.3.5 Staff code of conduct;

3.3.6 Whistleblowing policy;

3.3.7 Taking, storing and using images of children policy;

3.3.8 Data protection policy for staff;

3.3.9 School rules;

3.3.10 Mobile phone policy;

3.3.11 Behaviour management policy;

3.3.12 Relationships and sex education policy;

3.3.13 Staff handbook as follows:
(a) Section 6 – code of conduct for staff;
(b) Section 21 – whistleblowing policy;
(c) IT policy; and
(d) Social media policy

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 School reception 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:

5.2 References to the **Proprietor** are references to the Board of Governors.

5.3 Reference 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.

5.4 The Strategic Leadership Group (**SLG**) comprises Mr Graham Bone (Head), Mr Miles MacEacharn (Bursar), Mrs Saskia Van Schalkwyk (Head - Exeter Junior School), Miss Ali Dunning (Deputy Head – pupil development, welfare, and wellbeing and DSL), Mr Paul Fennemore (Deputy Head – academic), Miss Bethan Rose (Deputy Head - enrichment, character and community), Mrs Liz Williams (Director of External Relations), and the Head of HR.

5.5 The Senior School Leadership Team (**SSLT**) comprises Mr Graham Bone (Head), Mr Miles MacEacharn (Bursar), Miss Ali Dunning (Deputy Head – pupil development, welfare, and wellbeing and DSL), Mr Paul Fennemore (Deputy Head – academic), Miss Bethan Rose (Deputy Head - enrichment, character and community), plus Mr Luigi Chu (Assistant Head - Sixth Form), Mrs Julia Daybell (Assistant Head - Lower School), and Mr Mike Glanville (Assistant Head - Middle School)

5.6 The Junior School Leadership Team (**JSLT**) comprises Mrs Saskia Van Schalkwyk (Head - Exeter Junior School), Mr John Wood (Deputy Head - Exeter Junior School), Mr Rhys Evans (Head of Upper School - Exeter Junior School), Mrs Leah Hardy (Head of Lower School - Exeter Junior School), and Mr Dan Ayling (Head of Exeter Pre-Prep School).

5.7 The Operations Leadership Team (OLT) comprises Mr Miles MacEacharn (Bursar), Mrs Liz Williams (Director of External Relations), the Head of HR, Mrs Anya Rowley (Head of Finance), Mr Craig Stewart (Head of Operations), Mr Anthony Martin (Head of IT Services) and Mrs Alice Holohan (Director of Development and Alumni).

5.8 For this policy, **SLT** refers to **SLG**, **SSLT, JSLT** and **OLT** together.

5.9 The **SLT digital lead** is a member of the SLT with lead responsibility for the School's digital technology.

5.10 In considering the scope of the School's online safety strategy, 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**).

6 Responsibility statement and allocation of tasks

6.1 The Proprietor has overall responsibility for all matters which are the subject of this policy and for approving and reviewing its effectiveness.

6.2 The Proprietor 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 the Proprietor's response to this duty.

6.3 To ensure the efficient discharge of its responsibilities under this policy, the Proprietor has allocated the following tasks:

Task	Allocated to	When/frequency of review
Keeping the policy up to date and compliant with the law and best practice	Head of IT Services in conjunction with DSL	As required, and at least termly
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 taken in response and evaluating effectiveness	DSL	As required, and at least termly
Online safety	DSL	As required, and at least annually
Taking appropriate action to meet the Cyber security standards for schools and colleges[1]	Head of IT Services and DSL	As required, and at least annually
Assessing the School's approach to filtering and monitoring and assessing this in light of new or emerging risks and technologies	DSL, Head of IT Services, and Chair of Welfare and Safeguarding Committee	As required, and at least annually
Reviewing digital technology strategy	SLT digital lead	As required, and at least annually
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	DSL	As required, and at least annually
Formal annual review	Welfare and Safeguarding Committee	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 that it is applied and updated on a regular basis.

[1] The Cyber security standards for schools and colleges were developed to help schools improve their resilience against cyber-attacks. Broader guidance on cyber security including considerations for governors and trustees can be found at National Cyber Security Centre – NCSC.

7.1.2 The DSL 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 the filtering and monitoring systems in place in school.

7.1.3 The responsibility of the Designated Safeguarding Lead includes:

(a) 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 child protection and safeguarding policy and procedures;

(b) working with the SLT 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;

(c) working with the Head of IT Services 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.

(d) overseeing and acting on: filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems;

(e) overseeing and acting on: arrangements for information and cyber security and action taken to meet the Cyber security standards to protect the School from cyber-attacks and improve cyber resilience

(f) regularly monitoring the technology incident log maintained by the Head of IT Services to assess whether changes need to be made to the digital technology strategy and staff and pupil training;

(g) regularly updating other members of the School's Senior Leadership Team and the Proprietor on the operation of the School's safeguarding arrangements, including online safety practices;[2]

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

(i) promoting an awareness of and commitment to online safety education/awareness raising across the School and beyond.[3]

SLT digital lead

7.1.4 At Exeter School the role of SLT digital lead is taken by the IT Steering Group (ITSG). This consists of the Head, the Deputy Head (Academic), the Head of Technology for Learning, the Head of IT Services and the Bursar. The DSL and IT team members attend as required.

7.1.5 The SLT digital lead should have strategic oversight of all digital technology. They will create and manage the digital technology strategy led by the needs of staff and students.

7.1.6 The SLT digital lead will be accountable for:

(a) the delivery of the digital technology 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 or college;

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

(d) identifying and acting on digital technology training needs for staff and students.

7.1.7 The SLT digital lead will also be responsible for:

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

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

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

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

Head of IT Services

7.1.8 The Head of IT Services, together with their team, is responsible for the effective operation of the School's filtering system 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.

7.1.9 The Head of IT Services 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 or cyber-attack;

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

(c) filtering and monitoring systems are maintained, providing filtering and monitoring reports and completing actions following concerns or checks to systems;

(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.

7.1.10 The School has in place robust web filtering and monitoring which blocks access to harmful and adult content. Through daily reports on user activity, the DSL is alerted to any potential safeguarding issues and will put in place the necessary support and/or education for pupils. The Head of HR receives weekly reports on staff user activity and will follow up, as required, if any potential safeguarding issues are flagged.

7.1.11 The Head of IT Services will report regularly to the Senior Leadership Team on the operation of the School's technology. If the Head of IT Services has concerns about the functionality, effectiveness, appropriateness or use of technology within the School, including of the monitoring and filtering systems in place, he/she will escalate those concerns promptly to the Designated Safeguarding Lead.

7.1.12 The Head of IT Services is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's child protection and safeguarding policy and procedures.

7.2 **All staff**

7.2.1 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.

7.2.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.2.3 Training for 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.

7.2.4 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.

7.2.5 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;

(d) cyberbullying.

7.2.6 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.

7.2.7 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.

7.2.8 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*" 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.

7.2.9 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 incidents as a breach of discipline and will deal with them under the School's Behaviour management policy and also as a safeguarding matter under the School's Safeguarding and child protection policy and procedures.

7.2.10 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 and procedures. 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**.

7.3 Parents

7.3.1 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.

7.3.2 If parents have any concerns or require any information about online safety, they should contact their child's form tutor in the first instance.

8 Filtering and Monitoring

8.1 Whilst considering their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, the Proprietor will do all it reasonably can to limit pupil's exposure to risks from the School's IT system. As part of this process the School has appropriate filtering and monitoring systems in place for all pupils and staff when using the School Wi-Fi 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 and its effectiveness 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.[4]

8.4 The School manages access and restrictions to content across its systems for all users, including guest accounts. 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/learners, etc.) Safe search is enforced on all web traffic on site.

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.

[4] See Plan technology for your school (HM Government, September 2024) which includes a self-assessment tool to assist schools in meeting the filtering and monitoring standards

8.7 Access to content through non-browser services e.g. 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.

8.9 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;

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 and intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective IT Acceptable usage policy when using School technology. All such use is monitored by the IT team.

9.2 Pupils and staff require individual usernames 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 usernames or passwords must report it to the IT team immediately.

9.3 No laptop or other mobile electronic device may be connected to the School network without the consent of the Bursar or Head of IT Services. The use of any device connected to the School's network will be logged and monitored by the IT team. See also 9.5 below.

9.4 The School has a separate wireless network connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the wireless network. Use of this service will be logged and monitored by the IT team.

9.5 Inappropriate material

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

9.5.2 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 ever evolving issues but these can be classified into four main areas of risk:

(a) **Content** - being exposed to illegal, inappropriate or harmful content, including, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, 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** - online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as the 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, students or staff are at risk, it should be reported to the Anti-Phishing Working Group.

Use of mobile phones, electronic devices and smart technology

9.5.3 The School has adopted a mobile phone policy that prohibits pupils in Year 3 to Year 11 using mobile phones throughout the school day. This includes during lessons, the time between lessons, breaktimes and lunchtimes.

9.5.4 Whilst pupils in the sixth form are allowed to carry their phone during their day, its use is only permitted in certain spaces and at certain times, e.g., during social times and only in the sixth form centre / study area; or in certain lessons / activities at the teacher's discretion (e.g., fitness training in the gym, or creative arts lessons). Sixth form pupils are not allowed to record of photograph other pupils on their personal device and, if using a school device, any photo or video of other pupil(s) must be for an educational reason and with the other pupil(s)' permission. Sixth form pupils are reminded regularly of their responsibility to model good behaviour, and to be responsible.

9.5.5 The School rules about the use of mobile phones, 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 policy for pupils.

9.5.6 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.

9.5.7 The School does all that it reasonably can to limit children's exposure to the risks identified above through the use of the School's IT system, including robust activity logging procedures to monitor content and usage within the School to identify patterns of misuse or suspected misuse.

9.5.8 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email text messaging and social media sites) when they are using on Bring Your Own Devices (**BYOD**) (excluding mobile devices) and school devices that are connected to the School's network, and their effectiveness is regularly reviewed.

9.5.9 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 illegal, inappropriate or harmful content (including content created by generative AI tools in real-time). The School has adopted a policy of prohibiting pupils in years 3 to 11 from having mobile phones about their person during the school day as a mechanism to manage such risks.

9.5.10 The use of mobile electronic devices by staff is covered in the staff handbook. 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 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.

Misuse by pupils

10.2.1 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 management policy, including the anti-bullying policy where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-bullying	Form tutor Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead (DSL)
Sharing nudes and semi-nude images (sexting/youth produced sexual imagery)	Safeguarding and child protection policy	Head of section (Deputy DSL) or DSL
Sexual violence and sexual harassment (whether during or outside of school)	Safeguarding and child protection policy	Head of section (Deputy DSL) or DSL.
Harassment	Safeguarding and child protection policy	Form tutor Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Upskirting	Safeguarding and child protection policy	Head of section (Deputy DSL) or DSL
Radicalisation	Safeguarding and child protection policy	Head of section (Deputy DSL) or DSL.
Any action resulting in disruption to digital technology systems in school	IT strategy	Head of IT Services Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Other breach of IT Acceptable usage policy, including unauthorised use of mobile devices during teaching hours.	See relevant policy referred to in acceptable use policy	Form tutor Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead

10.2.2 **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.

10.3 **Misuse by staff**

10.3.1 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 allegations, which is set out in the Safeguarding and child protection policy and procedures.

10.3.2 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 their Head of Department/Line Manager in accordance with the staff whistleblowing policy; and

(b) Anyone else should speak to the Head.

10.4 **Misuse by any user**

10.4.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the Head of IT Services or the Designated Safeguarding Lead.

10.4.2 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.

10.4.3 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 (see the School's curriculum policy). 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 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching pupils:

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

11.3.2 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*";

11.3.3 to be critically aware of content they access online (including how to recognise illegal, inappropriate or harmful content) and guided to validate accuracy of information;

11.3.4 to be aware of and how to identify the risks posed by cybercrime;

11.3.5 how to recognise suspicious, bullying or extremist behaviour;

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

11.3.7 the consequences of negative online behaviour;

11.3.8 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

11.3.9 how to respond to harmful online challenges and hoaxes.

11.4 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.

11.5 Pupils are 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 Behaviour management policy and also as a safeguarding matter under the School's Safeguarding and child protection policy and procedures.

11.6 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

11.7 The School's IT Acceptable usage 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.

11.8 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, see School's safeguarding and child protection policy and procedures and relationships education/RSE/ PSHE/other curriculum policy.

11.9 Useful online safety resources for pupils

11.9.1 http://www.thinkuknow.co.uk/

11.9.2 http://www.childnet.com/young-people

11.9.3 https://www.saferinternet.org.uk/advice-centre/young-people

11.9.4 https://mysafetynet.org.uk

11.9.5 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

11.9.6 https://www.bbc.com/ownit

12 Training

12.1 Proprietor

12.1.1 To ensure that all Governors 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 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 strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy. Training specifically addresses the School's filtering and monitoring provisions in place, including activity logging and reporting mechanisms, 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-nude 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 Appendix 1 of the School's Safeguarding and Child Protection Policy and Procedures 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 through generative AI tools, and to 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/

(e) http://educateagainsthate.com/

(f) https://www.commonsense.org/education/

(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 (DSIT and UKCIS, March 2024)

(j) Using External Expertise to Enhance Online Safety Education(UKCIS, October 2022)

(k) Education for a connected world framework (UKCIS, June 2020)

(l) https://www.lgfl.net/online-safety/resource-centre

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

(n) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

(o) SELMA Hack online hate toolkit (SWGFL, May 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)

(r) Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.

(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

12.2.11 Devon council local safeguarding partnership has produced guidance for parents on radicalisation which is available here: Preventing Radicalisation - Safer Devon

12.3 Parents

12.3.1 The School is in regular contact with parents and carers and uses its 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.

12.3.2 Online safety resources and updates will be shared with parents on the dedicated online safety page on My School Portal and via newsletters and safeguarding bulletins. Parental Forum meetings and/or parent talks from external speakers will provide opportunity for interactive engagement regarding topical issues.

12.3.3 Parents are encouraged to read the IT Acceptable usage policy for pupils with their son/daughter to ensure that it is fully understood.

12.3.4 Parents have an important role in supporting the School's policy on prohibiting the use of mobile phones during teaching hours. 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.

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**

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

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

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

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

(i) http://www.askaboutgames.com

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

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

(l) LGfL: parents - scare or prepare

(m) Thinkuknow: what to do if there's a viral scare online

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 online) or "cyber dependent" (crimes that can be committed only by using a computer).

13.2 12.2 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 The School will take appropriate action to meet the Cyber security standards to improve resilience against cyber-attacks.

13.5 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 online and child sexual abuse and exploitation, nor other areas of concern such as online bullying or general online 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 face by their pupils.

14.2 Furthermore, 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 DSL who has 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 technology incident log by the Head of IT Services.

15.3 The records created in accordance 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 on its website privacy notices which explain how the School will use personal data.