

Online Safety Policy

Reviewed by: MHO/JSM September 2026
Approved by: Governors, September 2026

Next review by: September 2027



1 Introduction

- 1.1 Digital technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.
- 1.2 However, the use of these technologies can put young people at risk within and outside the school. The issues encompassed by the term 'online safety' are considerable and ever evolving, but can be categorised into four areas of risk:
- 1.2.1 **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories;
 - 1.2.2 **contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
 - 1.2.3 **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI, and online bullying; and
 - 1.2.4 **commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.
- 1.3 Many of these risks reflect situations in the offline world and it is essential that this Online Safety Policy is used in conjunction with other school policies such as the:
- Safeguarding (Child Protection) Policy
 - Acceptable Use of ICT for Staff Policy
 - Anti-Bullying Policy
 - Behaviour Policy
 - Code of Conduct for Pupil's Use of ICT
 - Code of Conduct for Staff
 - Data Protection Policy
 - Information Security Policy
- 1.4 This policy applies to all members of the School community (including staff, pupils, parents and visitors) who have access to the School's ICT facilities both in and out of the school. It also applies to behaviour related to online safety, such as cyberbullying, which may take place outside the school but which is linked to membership of the School. The School will address such behaviour in accordance with this policy and the Behaviour Policy.

2 Roles and Responsibilities

- 2.1 **The Governing Body**, through the Education Committee, is responsible for overseeing the School's approach to online safety and ensuring that appropriate filtering and monitoring systems are in place and that a review of their effectiveness is carried out at least once every academic year.
- 2.2 **The Designated Safeguarding Lead (DSL)** has lead responsibility for online safety within the School, including understanding the filtering and monitoring systems and processes in place, and is responsible for the content and delivery of online safety education for pupils, staff and parents and ensuring that this is kept up to date. The Designated Safeguarding Lead is also responsible for maintaining the online safety incident log and monitoring it for emerging patterns or trends. The Designated Safeguarding Lead is responsible for following up on any child protection issues that may arise out of an online safety incident in accordance with the School's Safeguarding (Child Protection) Policy.
- 2.3 **The Deputy Head (Pastoral)** is responsible for ensuring that online safety education is embedded in the PSHE and RSE curriculum to enable all pupils to develop an understanding of the risks as appropriate to their age and stage of development. They are responsible for monitoring its effectiveness, including via review of the online safety incident log in conjunction with the Designated Safeguarding Lead.
- 2.4 **The Director of Digital Strategy and IT** is responsible for ensuring that the School's technical infrastructure is as secure as possible; that only registered users may access the School's networks and devices; that appropriate filtering and monitoring systems are maintained and that use of the School's ICT facilities is regularly monitored to ensure compliance with Acceptable Use of ICT for Staff Policy. The Director of Digital Strategy and IT provides technical support to the Designated Safeguarding Lead in reviewing the effectiveness of the School's filtering and monitoring systems, including checking that filtering operates appropriately on all internet-connected devices in all relevant locations and ensuring that a record of these checks is retained.
- 2.5 **All staff** are responsible for ensuring that they have an up to date awareness of this policy, that they adhere to the School's Acceptable Use of ICT for Staff Policy and Information Security Policy, that they understand the expectations, roles and responsibilities relating to filtering and monitoring, that they report any suspected misuse or concerns relating to online safety, filtering or monitoring to the Deputy Head (Pastoral) and Designated Safeguarding Lead as appropriate and that they help pupils to understand the Online Safety Policy and related policies.
- 2.6 **Pupils** must engage with opportunities for learning about online safety and take responsibility for keeping themselves and others safe online both within and outside school. They must ensure they adhere to the Code of Conduct for Pupil's Use of ICT and understand the importance of reporting to a member of staff any abuse, misuse, inappropriate or harmful content or other online safety concern.
- 2.7 **Parents** are expected to support the School in promoting good online safety practice and to follow the guidelines in this policy and to support their child in understanding and following the School's expectations for safe and appropriate use of technology.

3 Reducing Online Risks

- 3.1 The online world is constantly evolving with new apps, devices, websites and material emerging all the time. The School will:

- 3.1.1 Ensure that appropriate filtering and monitoring systems are in place which:
 - (a) have clearly identified and assigned roles and responsibilities;
 - (b) are reviewed for effectiveness at least once every academic year;
 - (c) block harmful and inappropriate content without unreasonably affecting teaching and learning; and
 - (d) provide effective monitoring that meets the School's safeguarding needs.
- 3.1.2 Consider the educational benefits and online safety risks of emerging technologies, including generative AI, before allowing their use in school; and
- 3.1.3 Ensure, through online safety education and the School's policies and procedures, that pupils, staff and parents understand the School's expectations regarding safe and acceptable online behaviour both within and outside school.

4 Pupil Education and Information

- 4.1 All new pupils receive a copy of the School's Code of Conduct for Pupils' Use of ICT. They are expected to discuss its contents with a parent or teacher and then confirm that they will adhere to its terms.
- 4.2 The School's PSHE and RSE programmes include comprehensive online safety provision, which is age and developmentally appropriate and, where necessary, tailored to pupils' individual needs and vulnerabilities. A summary of the Scheme of Work is included in the **Digital Safety Booklet**, and topic overviews are included in the appendices to the School's PSHE and RSE Policy, with a more detailed version available to staff.
- 4.3 Key online safety messages are delivered through the personal development curriculum, including assemblies and/or form time. External speakers may also be invited to speak to pupils, and sometimes parents, on online safety topics, in accordance with the School's Visitor Procedures.

5 Staff Awareness

- 5.1 All new members of staff receive training on the School's Online Safety Policy and Acceptable Use of ICT for Staff Policy as part of their safeguarding induction. This includes an understanding of the expectations, applicable roles and responsibilities relating to filtering and monitoring. They are also given a copy of the **Digital Safety Booklet**.
- 5.2 All staff receive information about online safety issues at staff meetings as and when required and as part of their regular safeguarding training updates. Online safety updates are provided as required and at least annually. The Digital Safety Booklet is updated every year and is sent out to all staff as a link, or via the minutes of staff meetings.

6 Engagement with Parents

- 6.1 The **Digital Safety Booklet** is updated every year and sent out annually at the start of the academic year usually via email. The School also provides parents with information about the filtering and monitoring systems it uses and reinforces the importance of children staying safe online, including information about the online activities, websites and services pupils may be asked to use.
- 6.2 Parents are invited to attend events relating to online safety such as webinars led by members of staff and external speakers.

7 Use of Technology in School

- 7.1 **Acceptable Use Agreements:** All use of the School network, personal devices in school and devices owned by the School (whether on or off the School site) must comply with the Acceptable Use of ICT for Staff Policy or the Code of Conduct for Pupils' Use of ICT as applicable. Any devices used during the school day must access the internet via the School's wireless network and 'hot-spotting' via a mobile phone is strictly prohibited for staff and pupils unless explicit permission is given, in exceptional circumstances, by the Director of Digital Strategy and IT or the Designated Safeguarding Lead. Failure to comply with the relevant Acceptable Use agreement may result in disciplinary sanctions for pupils in accordance with the School's Behaviour Policy and for staff under the School's Disciplinary Procedure.
- 7.2 **Devices owned by the School** may be assigned to staff or pupils for short-term or longer-term use. Devices assigned for short-term use (for example in a particular lesson, for an exam or on a school visit) must be signed in and out by the member of staff responsible. Devices assigned for longer-term use are subject to a separate agreement which must be signed by the member of staff or pupil at the time the devices are issued.
- 7.3 **Personal Devices** may not be used by pupils in the Lower and Middle School during the school day without the express permission of a member of staff. Sixth Form pupils have permission to use personal devices with certain restrictions (see the School's Behaviour Policy and Mobile Phone Guidance). Pupils must not have any device capable of mobile communication in examinations as this will result in disqualification. If a personal device is deemed by a member of staff to be causing a distraction around the school, it may be confiscated until the end of the school day.
- 7.4 **Wearable Technology** includes electronics that can be worn on the body, either as an accessory or as part of clothing, and can communicate, record, store or exchange data. If wearable technology is worn in lessons or in public areas around the school, then the 'do not disturb' or 'flight' mode must be activated. Its use must also comply with paragraph 7.3, the School's Behaviour Policy and Mobile Phone Guidance.

8 Technical Infrastructure

- 8.1 The IT Management Team reviews and audits the safety and security of the School's technical systems. This will periodically be supplemented by an external audit and review.
- 8.2 Servers, wireless systems and cabling are securely located and physical access is restricted.
- 8.3 All users are provided with a username and password by the IT Department. Users are responsible for the security of their username and password. Multi-factor authentication (MFA) is enabled for staff accounts with access to cloud services or remote access to the School's systems and for IT administrative accounts.

9 Filtering and Monitoring

- 9.1 As part of its safeguarding duty, and in line with DfE guidance Keeping Children Safe in Education, the School has put in place appropriate filtering and monitoring systems to limit pupils' exposure to harmful and inappropriate online material when using the IT facilities and internet in school and when accessing the School's devices and systems outside school. The effectiveness of these systems is reviewed at least once every academic year by the Designated Safeguarding Lead and the Director of Digital Strategy

and IT, with involvement from the responsible governor. The review includes checks that filtering operates appropriately on all internet-connected devices in all relevant locations, and a record is kept of the checks undertaken.

- 9.2 The School's filtering system is designed to block harmful and inappropriate content without unreasonably impacting teaching and learning. Instant messaging and social networking sites, as well as gaming and other similar sites, will be blocked unless specifically authorised by the IT Management Team and the Assistant Head responsible for Teaching and Learning, in discussion with the Designated Safeguarding Lead. Controls for Sixth Form users may be less stringent than for pupils in the Lower and Middle School, provided that the filtering and monitoring arrangements remain appropriate for the age and ability of users and the School's identified safeguarding risks.
- 9.3 The School uses specialist filtering and monitoring software to provide information and alerts on pupils' network activity and behaviour that might constitute a safeguarding concern. The Designated Safeguarding Lead reviews this information at least daily (on school working days) and high-risk safeguarding alerts are reported promptly for appropriate action. Any potential concerns are evaluated to ensure that they are addressed appropriately. NB - Alerts received outside school hours or in school holidays may not be picked up until the next school working day and parents are made aware of this via the iPad Guidance for Parents and Surface Guidance for Parents.
- 9.4 The School's filtering and monitoring systems are designed to support child safeguarding. Parents are given access to the School's filtering and monitoring system outside school hours, enabling them to apply additional filters and monitor their child's online activity on their School-issued device. However, parents remain primarily responsible for supervising their child's independent online activity outside school, including use of personal devices and home networks.
- 9.5 Personal data is collected, processed, stored and transferred in accordance with data protection legislation and the School's policies (see the Data Protection Policy and relevant privacy notices for more information). The School carries out appropriate data protection impact assessments (DPIA) in relation to its filtering and monitoring arrangements and reviews the privacy information provided by relevant third-party providers.
- 9.6 All staff must know how to report and record concerns relating to filtering and monitoring, in accordance with the reporting arrangements set out in this policy and the School's Acceptable Use of ICT for Staff Policy.

10 Social Media

- 10.1 Social media applications include, but are not limited to: blogs; wikis; social networking sites; online discussion forums; collaborative spaces; online gaming; apps; video/photo sharing services (e.g. Instagram/Youtube/TikTok); chatrooms; instant messenger; and 'micro blogging' applications.
- 10.2 If a member of staff considers that access to a social networking site would be appropriate for staff or a group of pupils for curricular or extra-curricular purposes, a proposal must be submitted to the IT Network Manager, the Designated Safeguarding Lead and the Assistant Head responsible for Teaching and Learning, and authorisation must be received in advance. The use of social networking sites within school will only be permitted in appropriately controlled situations. Staff and pupils should not access social networking sites for personal use during school hours.

- 10.3 The safe and responsible use of social media is discussed with all new staff as part of their induction and is revisited with all staff during safeguarding training updates. Safe and professional behaviour is outlined for all staff in the Acceptable Use of ICT for Staff Policy and the Code of Conduct for Staff.
- 10.4 Safe and appropriate use of social media is taught to pupils as part of online safety education, in an age and developmentally appropriate way.

11 Artificial Intelligence (AI)

- 11.1 Pupils have access to a school-approved generative AI platform on their school devices. The only generative AI currently approved is Securly AI Chat, which is filtered and monitored through the School's filtering and monitoring platform. Any other generative AI platform for use by pupils must be approved by the Designated Safeguarding Lead and the Director of Digital Strategy and IT, and must be filtered and monitored. Pupils should not be able to access other generative AI platforms on their school devices.
- 11.2 Personal or confidential information must not be entered into generative AI tools unless the tool has been approved by the School for that purpose and its use complies with the School's Data Protection Policy, Information Security Policy, Acceptable Use of ICT Policy and Code of Conduct for Pupils' Use of ICT. Special Category Data, criminal offence data and safeguarding information must not be entered into any generative AI tool. Information entered into some generative AI tools may be collected, stored, shared or used to train or improve the tool.
- 11.3 Generative AI may produce inaccurate, incomplete, biased or misleading information. All users must check AI-generated information against reliable sources and must not rely on it as fact. Generative AI tools must not be used as a substitute for appropriate professional advice or support concerning health, medical or wellbeing issues, safeguarding concerns or other personal matters.
- 11.4 Pupils are educated about the risks and the safe, responsible and effective use of generative AI as part of the Personal Development Curriculum. Details of specific topics can be found in the School's PSHE and RSE policies.

12 Procedures for dealing with online safety incidents involving pupils

- 12.1 If a pupil feels uncomfortable or worried by anything online or on a device, they should tell a member of staff or parent as soon as possible.
- 12.2 Any allegation, complaint, concern or suspicion that a pupil has been involved in any of the following should be reported immediately to the Designated Safeguarding Lead and action will be taken in accordance with the School's Safeguarding (Child Protection) Policy:
 - 12.2.1 Possession of, or access or attempted access to a website containing images of child sexual abuse;
 - 12.2.2 Possession of, or access or attempted access to a website containing, illegal (eg obscene or criminally racist) or terrorist or extremist material;
 - 12.2.3 Any incident by electronic means involving 'grooming' behaviour;
 - 12.2.4 Any other incident (which may include cyber-bullying, the making or sharing of nudes and semi-nudes, including those generated using AI, or child on child

abuse) that suggests that a pupil or another child has suffered or is at risk of suffering harm.

- 12.3 Any concern or allegation regarding the making or sharing of nudes or semi-nude images including those generated using AI, must be reported to the Designated Safeguarding Lead immediately. All such incidents require a proportionate safeguarding response, whether the sharing is consensual or non-consensual. Staff must not view, copy, print, share, store or save the imagery themselves, or ask a child to share or download it, as this is illegal (if the image is viewed by accident this must be reported immediately to the DSL). Staff should not investigate the incident themselves or delete, or ask the child to delete, the image. The child should not be blamed or shamed but should be told that the incident will need to be reported to the Designated Safeguarding Lead and that they will receive support and help. Action will be taken in accordance with the School's Safeguarding (Child Protection) Policy, taking into account guidance published by the UK Council for Internet Safety: '*Sharing nudes and semi-nudes: advice for education settings working with children and young people*'. Incidents involving the making or sharing of nudes or semi-nudes will also be recorded by the Designated Safeguarding or Deputy DSL on the School's online safety incident log.
- 12.4 For guidance on collecting and preserving electronic evidence in other instances, particularly, where there has been an allegation of cyber-bullying, see Appendix 1 to this policy. The IT Management Team can also be consulted to assist in establishing, capturing or preserving relevant data or other evidence.
- 12.5 Any allegation of cyber-bullying which does not fall within 11.2.4 above should be reported to the Deputy Head (Pastoral) as soon as possible. Cyber-bullying incidents will be dealt with in accordance with the School's Anti-Bullying and Behaviour policies unless there is a risk of harm to a child and/or the incident constitutes child on child abuse, in which case it will also be dealt with under the School's Safeguarding (Child Protection) Policy.
- 12.6 Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft, unlicensed use of software or unlawful use of personal data should be reported to the Deputy Head (Pastoral). Such concerns will be managed in accordance with the School's Behaviour Policy although referrals may be made to outside agencies as appropriate.
- 12.7 Where there are reasonable grounds to suspect that illegal activity has taken place, the School will contact the police using 101, or 999 if there is immediate danger or risk of harm.
- 12.8 Any other misuse of the School's ICT facilities not falling within one of the categories above should be referred to the Deputy Head (Pastoral) who will take action as appropriate in accordance with the School's Behaviour Policy.

13 Procedures for dealing with online safety incidents involving staff

- 13.1 Any allegation, complaint, concern or suspicion that a member of staff has been involved in any of the following and which may meet the harm threshold, should be reported immediately to the Head (or to the Chair of Governors if the Head is the subject of the concern) and action will be taken in accordance with the School's Safeguarding (Child Protection) Policy, Appendix 6:

- 13.1.1 Possession of, or access or attempted access to a website containing, images of child sexual abuse;
 - 13.1.2 Possession of, or access or attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;
 - 13.1.3 Any incident by electronic means involving 'grooming' behaviour; and
 - 13.1.4 Any other incident that suggests that a pupil or another child has suffered or is at risk of suffering harm from a member of staff.
- 13.2 Any concern about a member of staff which does not meet the harm threshold must be reported and dealt with in accordance with the low-level concerns procedure set out in the School's Safeguarding (Child Protection) Policy.
- 13.3 Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft or unlawful use of personal data should be reported to the Head or the Bursar immediately. Such concerns will be managed in accordance with the School's Whistleblowing Policy and disciplinary procedures and will be referred to the police as appropriate.
- 13.4 Any other misuse of the School's ICT facilities not falling within one of the categories above should be referred to the Bursar who will take action as appropriate in accordance with the School's disciplinary procedures.

14 Monitoring and Review

- 14.1 This policy and the School's overall approach to online safety will be reviewed at least annually, supported by an annual risk assessment that considers and reflects the online risks faced by pupils, and in response to any new guidance or legislation, significant developments in technology or following a significant online safety incident.

Appendix 1: The collection and preservation of evidence

If you suspect that there are nudes or semi-nudes of a pupil or another child, including those generated using AI on a device, you should not attempt to search for or print off such images. You must not intentionally view, copy, print, share, store or save the imagery, or ask a child to share or download it. The device should instead be confiscated, secured and handed directly to the Designated Safeguarding Lead. The following applies to situations which do not fall into this category.

Preserve the evidence

Advise pupils and staff to try to keep a record of the abuse/misuse, particularly the date and time, the content of the message(s), and where possible a sender's ID (eg username, email, mobile phone number, IP address) or the web address of the profile/content. For example, taking an accurate copy or recording of the whole webpage address will help the service provider to locate the relevant content. Keeping the evidence will help in any investigation by the service provider, but it can also be useful in showing what has happened to those who may need to know, including parents, teachers, pastoral staff and the police. These steps must not be used to copy, save or otherwise reproduce nudes or semi-nudes of a child; the procedure above must be followed instead.

How to do this

It is always useful to keep a written record, but it is better to save evidence on the device itself, subject to the restrictions above.

Mobile Phones

Ensure the recipient keeps/saves any messages, whether voice, image or text. Unfortunately forwarding messages, e.g. to a teacher's phone, can result in loss of information from the original message, such as the sender's phone number.

Instant Messaging (IM)

Some services allow the user to record all conversations. The user could also copy and paste, and save these. Copied and pasted conversations can be edited so are less useful as evidence to the service provider or the police. Conversations recorded/archived by the IM service are better for evidence here. Conversations can also be retained electronically and, where appropriate, sections can be saved as a screen-grab.

Social Networking

On social networking sites, video hosting sites, or other websites, keep the site link, and, where appropriate, take a screenshot of the relevant content, ensuring that identifying information and the web address are retained where possible.

Chatrooms

Retain the conversation where possible or, where appropriate, take a screenshot of the relevant content, ensuring that identifying information is retained.

Email

The recipient should save the original email and, where appropriate, forward the message on to the staff member investigating the incident. They should be encouraged to save any subsequent messages. Preserving the whole message, not just the text, is more useful as this will contain 'headers' (information about the source of the message). Emails containing nudes or semi-nudes of a child must not be forwarded and must instead be reported immediately to the Designated Safeguarding Lead in accordance with the procedure above.

Threats

Use the 'Report abuse' or equivalent reporting function provided by social networking or other online services. Pupils and parents can make a report to CEOP where there are concerns about online sexual abuse or exploitation. Threatening phone messages should be preserved and depending on the nature and tone of the threats made, parents should consider contacting the police at an early opportunity in order to get the best advice. The School should also be informed as soon as possible so that appropriate safeguarding and pastoral support can be put in place for the pupil, with information shared with staff on a need-to-know basis.