



Reviewed – September 2026

Next review – September 2027

Online safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones, tablets and smartwatches
- Internet communications: email and IM
- Webcams and video conferencing
- Wireless games consoles

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This Online Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to online safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

1.0 WHAT ARE THE RISKS

- Receiving inappropriate content
- Radicalisation
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft; publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches

- Corruption or misuse of data
- Misinformation
- Disinformation (fake news)
- Conspiracy theories

As online safety is a relatively new concept and covers a wider scope than Internet use, a summary of a school's online safety responsibilities is outlined below. This list will assist in developing a coordinated and effective approach to managing online safety issues.

- The school IT Manager is **Mohammad Ghanty**, who will oversee and manage the school IT system, including security.
- The Online Safety Lead and Designated Safeguarding Lead – **Melanie Hodgson**
- The Online Safety Lead will seek advice from the UK Safer Internet Centre and, where concerns relate to child protection, CEOP. Where necessary, the police will also be consulted.
- The Online Safety Lead should maintain the Online Safety Policy, manage online safety training and keep abreast of local and national online safety awareness campaigns.
- The school will review the policy regularly and revise it annually to ensure that it is updated and considers any emerging technologies.
- The school will update its filtering systems regularly to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- The school will include online safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.
- All staff must read, understand and implement the Policy.
- The Online Safety Policy will be made available to all staff, Trustees, parents and visitors through the learning platform and website.

Implementation and Compliance

No policy can protect pupils without effective implementation. Staff must remain vigilant in planning and supervising appropriate, educational ICT experiences

2.0 Teaching and learning

Why is Internet use important?

Developing effective practice in Internet use for teaching and learning is essential.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Internet use is part of the statutory curriculum and a necessary tool for learning.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.1 Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

2.2 Local Area Network Security

- Users must act reasonably
- Users must take responsibility for their network use. For all staff, deliberately breaking or ignoring the school's electronic use policy is a disciplinary matter and may result in dismissal.
- Workstations should be secured against user mistakes and deliberate actions, e.g., deleting files and folders.
- Servers will be located securely and physical access restricted.
- The server operating system will be secured and kept up to date.
- Virus protection for the whole network will be installed and current.
- Access by wireless devices must be proactively managed.

2.3 Wide Area Network (WAN) Security

Firewalls and switches are configured to prevent unauthorised access.

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet should be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The IT Manager will review system capacity regularly.

2.4 Emails

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

2.5 School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The head teacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.
- The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

2.6 Use of Images

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website or any other published platform, particularly in association with photographs.
- Written permission from parents or carers must be obtained before any images of pupils are taken for school purposes, electronically published, or shared in any school communications including newsletters, social media or the school website. This permission is sought annually via the school's parental consent form.

2.7 Social Networking

- The schools will block/filter access to social networking sites.
- Online forums and discussion boards will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messaging and e-mail addresses, full names of friends, specific interests and clubs, etc.
- Pupils should be advised not to place personal photos on any social network space.
- They should consider how public the information is and consider using private areas.
- Advice should be given regarding background details in a photograph that could identify the student or his/her location, e.g., house number, street name or school.
- Teachers should be advised not to run social network spaces for student use on a personal basis.

2.8 Use of Generative AI and Monitoring

In line with the DfE's Generative AI: Product Safety Expectations and the current version of Keeping Children Safe in Education, the school recognises the increasing use of AI tools in education. Any generative AI applications (e.g., chatbots, image/video generators) must be pre-approved by SLT and used only under appropriate supervision. The school uses Impero to ensure effective filtering and monitoring of online activity, including AI tool usage. Impero alerts are regularly reviewed by designated staff to detect and respond to any potential misuse or exposure to harmful content. Staff and students are expected to use AI responsibly and in accordance with safeguarding, data protection, and online safety policies.

3.0 Social networking between staff and pupils in and out of school

In relation to social media (such as Facebook, Instagram, TikTok, Snapchat, X and WhatsApp), staff must not:

- Exchange accounts with pupils
- Add pupils to their account as "friends" or encourage them to do so
- Enter chat rooms with pupils
- Correspond with pupils using personal email addresses, e.g., Gmail, Hotmail and Yahoo
- Exchange personal mobile phone numbers with pupils
- Take photographs or videos of pupils without parent/guardian consent
- Take photographs or videos of pupils for non-school purposes
- Send or exchange images or videos of school staff, pupils or any aspect of school operations without authorisation or approval
- Download and store inappropriate images or other inappropriate material on teachers laptop/computers (if applicable) outside school hours and off school sites.
- No school devices are to be taken off site by teachers or children
- Access social media on any school device in the presence of pupils or without prior permission from SLT

One of the aims of the above is to prevent undue or inappropriate communication between pupils and staff. Anything that may lead to this, and not mentioned above, is also prohibited.

Failure to comply will result in a breach of Child Protection and Safeguarding Policy and will be dealt with accordingly.

Filtering and Monitoring

- The school's filtering and monitoring arrangements are informed by the DfE Filtering and Monitoring Standards, and are reviewed for effectiveness at least annually in line with the current version of Keeping Children Safe in Education. Melanie Hodgson (Online Safety Lead and Designated Safeguarding Lead) is responsible for the day-to-day oversight of filtering and monitoring, including weekly checks of the school's filtering software (Impero) to identify any breach in internet use throughout the school. Each check is recorded on the Filtering and Monitoring log, with any necessary actions noted and followed up.
- The Trustee with designated safeguarding oversight holds Trustee-level responsibility for filtering and monitoring, ensuring the school's arrangements remain compliant with the DfE Filtering and Monitoring Standards and KCSIE requirements.
- The school will work with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Online Safety Lead.
- This task requires both educational and technical experience.
- The filtering and monitoring system will be reviewed for effectiveness at least once a year. This review will assess the system against the DfE Filtering and Monitoring Standards and the findings will be reported to the Trustee with designated safeguarding oversight. Where online concerns are identified through monitoring, these are transferred into the appropriate behaviour or safeguarding log in line with the school's Behaviour Policy and Child Protection and Safeguarding Policy.

Emerging Technologies

- Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school.
- Mobile phones are not allowed during school time by pupils. The sending of abusive or inappropriate text messages is forbidden.

3.2 Cyber Security

The school recognises that cyber security incidents, including data breaches, ransomware, and unauthorised access to school systems, can pose a safeguarding risk. The IT Manager is responsible for maintaining the security of school systems. Any suspected cyber security incident must be reported to the IT Manager and DSL immediately.

4.0 Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
- On joining the school, parents and carers are provided with the school's Google Workspace for Education (GAfE) information form, which outlines how online learning platforms are used. Written consent is obtained from parents and carers for the use and publication of their child's images in school communications, the website and other platforms. Parents and carers have the right to withdraw image consent at any time by contacting the school office in writing. All staff are required to read the school's Acceptable Use Agreement (AUP). Pupils are taught the principles of acceptable and responsible use of school ICT systems and the internet through their computing lessons and the school's online safety curriculum."

Internet Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

4.2 Pupil Mobile Phones and Devices

The school does not permit pupils to bring mobile phones or any mobile devices into school. In the event that a device is brought in, it will be confiscated and returned to parents/carers at the end of the day. The school recognises that incidents involving the sending or posting of nude or semi-nude images between children — including AI-generated or digitally altered images (deepfakes) — may occur outside of school. Any such incidents that come to the attention of the school will be treated as a safeguarding matter and responded to in line with the Child Protection and Safeguarding Policy and the current version of Keeping Children Safe in Education.

5.0 Use of Personal Mobile Phones — All Staff (including Early Years)

The school recognises that personal mobile phones have the potential to be used inappropriately. Personal mobile phones should not generally be needed or used during the school day. Where they must be kept on the premises, they should be stored safely in staff bags at all times during working hours.

Staff must not:

- Use mobile phones in the presence of children or during lesson times
- Use mobile phones to take photographs or videos of children
- Give their mobile phone number to any pupil, including past pupils under the age of 18
- Access their mobile phone during working hours except during a designated break, which must be away from children

Mobile phones may be used on school trips for communication between staff only.

During working hours, mobile phones must be either switched off or on silent. Mobile phones can only be used on a designated break, and this must be away from the children

CCTV

See CCTV policy

Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher, unless it is the head teacher, in which case complaints will be sent to the Chair of Trustees.
- Pupils and parents will be informed of the complaints procedure via the Concerns and Complaints Policy
- Parents and pupils will need to work in partnership with staff to resolve issues.

Awareness of the policy

- Safety rules will be posted around the school.
- Pupils will be informed that network and Internet use will be monitored.
- Safety training will take place regularly to raise awareness of the importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An online safety module will be included as part of the Computing curriculum.
- All staff will have access to the School Online Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct are essential.

- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Parents' attention will be drawn to the school's Online Safety Policy on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

Websites Offering Additional Advice and Guidance

Thinkuknow (CEOP education programme) — <https://www.thinkuknow.co.uk>

CEOP Education (resources for schools) — <https://www.ceopeducation.co.uk>

CEOP Safety Centre (report online abuse or grooming) — <https://www.ceop.police.uk/safety-centre>

Childline — <https://www.childline.org.uk>

NSPCC – Online Safety — <https://www.nspcc.org.uk/keeping-children-safe/online-safety>

Internet Watch Foundation — <https://www.iwf.org.uk>

UK Safer Internet Centre — <https://saferinternet.org.uk>

Internet Matters — <https://www.internetmatters.org>