



Online Safety Policy

Approved by:	Headteacher	Date: December 2025
Last reviewed on:	December 2025	
Next review due by:	December 2026 (annual)	

Writing and reviewing the Online Safety Policy

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, mobile phones, staff code of conduct and anti-bullying.

- The school has an Online Safety Leader and this person is also the Designated Safeguarding Lead as the roles overlap. This person is Julia Waterson.
- The policy has been written by the school, building on best practice and government guidance. It has been agreed by the Leadership Team and approved by governors
- The policy and its implementation will be reviewed every 2 years.

Teaching and learning

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children
- The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- Children will be taught to be critically aware of the materials they read
- Children will be taught how to evaluate whether a website is useful and appropriate for the task and will be taught what to do if they or another child comes across inappropriate material (See 'Rules' in the Appendix)

Managing online access and security

The school will provide managed online access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when online and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium. (Talk Straight)
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system (SENSO) which is regularly checked to ensure that it is working, effective and reasonable
- The filtering system will be checked through a reporting procedure, which the Online Safety Leader will monitor very regularly
- If staff or children come across unsuitable on-line materials, the site must be reported to the Online Safety Leader
- Any problems arising in school should be reported to the Online Safety Leader
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by passwords
- Systems will be in place to ensure that online use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform Online safety policy.
- The security of school IT systems will be reviewed regularly.

Social Networking and Online Activity

- Children are taught not to reveal personal details about themselves or others in communication, or arrange to meet anyone without specific permission
- Staff to child email communication must only take place via a school email address and with the parents' knowledge that the e-mail exchange is taking place
- Staff do not reply to children's email unless they copy the parent in as well
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community. (Staff code of conduct outlines clear expectations)

Published content and the school website

- The contact details on the website should be the school address, email and telephone number
- The head teacher or any designated staff will take overall editorial responsibility and ensure that content is accurate and appropriate
- All staff will endeavour to ensure that content added to the website is appropriate and accurate, including messages to parents
- The website content will be updated and maintained by authorised individuals who will have their own identification and password in order to be able to access the site
- Images/footage of children in any media will only be used where consent has been given by parents on our 'Permission' form

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the Online safety policy and the staff code of conduct.
- Staff must not store images of pupils or pupil personal data on personal devices
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business

Using Mobile Phones (See more details in separate policy)

- Only children in Years 5 and 6 may bring mobile phones in to school. Parents need to have read and signed the mobile phone consent policy.
- Mobile phones must be handed to the class teacher at the beginning of the day, where they will be stored in a safe place, and remain switched off until the end of the school day
- School cannot be held responsible for the loss of or damage to children's own mobile phones
- Responsible use of mobiles will be included in the PSHE/computing programme, including cyberbullying and appropriate use of text and photos
- As with email, children will be taught to save inappropriate messages and told not to respond; they will be encouraged to show a parent when at home or an adult when in school, if they receive anything inappropriate or offensive
- Staff will, where possible, use a school phone where contact with parents is required

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) which came into force on May 25, 2018

Policy Decisions

Authorising access

- All staff must read and sign the staff code of conduct which includes information about using the internet
- All children will have their own password to access the internet
- Online access will be supervised with filters in place

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access
- The school will monitor ICT use to establish if the Online Safety Policy is adequate and that the implementation is appropriate and effective

Handling Online safety complaints/concerns

- Children should be encouraged to report any issues/concerns to parents when at home or adults in school
- KS2 children will be taught how to report concerns to the Child Exploitation and Online Protection agency (CEOP). The Childline number is also visible around the school.
- If any member of staff receives a report of an issue (from a child or parent), it should be recorded (Appendix 2) and shared with either the Online Safety Leader. If the staff member assesses it to be of a safeguarding nature, they should go straight to one of the DSLs.
- The Online Safety Leader will consider the best course of action which will often involve contacting parents
- Children and parents will be informed of consequences for children misusing the internet
- Any complaint about staff misuse must be referred to the Headteacher
- Any complaint about misuse by the Headteacher must be referred to the Chair of Governors – contact details can be found in the Child Protection and Safeguarding Policy
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures
- For incidents which involve youth produced sexual imagery (sexting), or allegations of Peer on Peer abuse, please refer to the Child Protection and Safeguarding Policy

Communication of the policy

To children

- Appropriate elements of the Online Safety Policy will be shared with children
- Online safety rules will be shared with the children and regular reminders will be given in lessons
- Children will be informed that network and online use will be monitored
- Curriculum opportunities to gain awareness of online safety issues, and how best to deal with them, will be provided for children. This should be addressed each year as children become more mature and the nature of newer risks can be identified

To staff

- All staff, as part of their induction, should read the school's Online Safety Policy
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will either be supervised by senior management or be on the Leadership Team. They will follow clear procedures for reporting issues.
- Staff are not permitted to use school devices to access chat rooms or social networking sites in school. Twitter is the exception for professional use.

- Staff must adopt the same level of professionalism when online at home for personal use as they do at school, this includes keeping staff and children's names and details confidential
- Staff are encouraged to check the security settings on their own personal profiles on social networking sites and ensure that the general public can only access a 'limited' amount of information
- Parents are able to contact staff and teachers on school email accounts
- Staff will report any offensive emails to the head teacher
- Staff should ensure that computers are either locked or logged off when not in use
- All staff are expected to read and sign the staff code of conduct which includes 'On line user expectations'

To Parents/Carers

- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters and on the school website where there is a page on 'Online safety' with a range of useful resources and links
- The school run Online safety training for parents, with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust
- Parents should be encouraged, where possible, to interact with their children on the internet as well as provide other opportunities for learning and recreation
- It is ultimately a parent's responsibility to closely monitor their child's use of technology outside of school - including use of mobile phones, the internet etc. If they have evidence of cyber-bullying involving school children and feel unable to resolve the matter themselves, they should liaise directly with the school (normally via the class teacher first) about how best to proceed

Linked policies/procedures

Anti-Bullying	Complaints Procedure (responding to Parents concerns)
Child Protection and Safeguarding	Staff Acceptable Use Agreement – a part of the code of conduct



Appendix 1

Kingswood Online Safety

Tell an adult – You should always tell an adult if you come across something inappropriate, or that worries you, while using technology. Even if you are just a little unsure, an adult will be able to give you good advice.

How would you feel? - Everyone deserves to be able to enjoy technology without getting nasty messages or emails. Bullying by using technology is no more acceptable than bullying in person. How would you feel if someone wrote you a nasty message?

Is it appropriate? When you go to a website, ask yourself if it is appropriate. If you would not show it to a teacher or someone at home, it probably is not! If it is inappropriate, close it straight away and tell an adult.

Never give out details. Unless an adult has specifically asked you to, you should not be contacting anyone that you do not know on the internet or by mobile phone. Whoever you are talking to, even if you think you know them, you should not be giving out personal details, or arranging to meet anyone.

Know the rules! The school rules, and any rules that you follow at home, are there to protect you and help you stay safe when using technology. Make sure you know the rules and follow them at all times.

THINK!

Kingswood Online Safety Rules

These rules help me to stay safe on the internet

- I will only use the internet when there is an adult present
- I will keep personal details to myself and I will not share them with other people. E.g. my password or home address
- I will tell an adult immediately if I receive a message, or see something on the screen that makes me feel uncomfortable or upset
- I will always be polite and kind when I write and send messages
- I will only communicate with people I know or that a responsible adult has approved
- I will look after equipment each time I use it

THINK

Kingswood Primary School Online Incident Form

Child's name:	Location:	
Year group:	Date:	Time:

Details of the incident (website/device/evidence from SENSO monitoring system):

Actions taken/follow up:

Adult name:	Position:
Date:	Signed:

Adult name:	Position:
Date:	Signed: