Beachborough School

Online Safety Policy

Updated: September 2026

Date of next Review: September 2027

Policy Lead: Head of Computing & Ms S J Lapper (Deputy Head - DSL)

Reviewed by: Senior Leadership Group

Statutory Guidance:

This policy has regard to:

- Keeping Children Safe in Education
- Working Together to Safeguard Children
- The Prevent Duty Guidance
- DfE Filtering and Monitoring Standards
- UKCIS Education for a Connected World Framework
- The Independent School Standards Regulations
- EYFS Safeguarding and Welfare Requirements

Aims:

Beachborough aims to:

- Ensure secure and supervised access to information and communication technology (ICT) for all pupils
- Encourage pupils to use technology to support their learning
- Promote digital safety, wellbeing and responsible use of technology
- Encourage all members of the community to gain a healthy balance of ICT use in both school and at home.

Beachborough recognises the importance of mobile devices and computers for communication and education as well as for recreation and socialising. However, we also recognise that some individuals may use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Students may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity. Abuse can take place wholly online and may be used to facilitate offline abuse. Children may also use these technologies in a way that leaves them vulnerable.

Beachborough educates pupils about e-safety issues across all curriculum subjects, but particularly in the following ways:

- PSHE lessons
- Computing lessons
- Age-specific assemblies

It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our effective whole school approach to online safety empowers us to protect and educate pupils in their use of technology and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into **four areas of risk**:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; 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.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non- consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Artificial Intelligence (AI):

Artificial Intelligence (AI) is increasingly present in online tools, apps, and educational platforms used by children. While AI can enhance learning and engagement, it also presents risks such as exposure to inappropriate content including AI generated images and content, misinformation, disinformation, biased information, data privacy concerns, cybercrime, fraud and unmonitored interactions (e.g. with AI chatbots). To mitigate these risks, the school will ensure that only age-appropriate, teacher-approved AI tools are used under adult supervision. AI systems will be evaluated for safety, data protection compliance, and educational value. Children will be taught, in an age-appropriate way, how to use AI responsibly and to always seek help from a trusted adult if they are unsure or feel uncomfortable.

As a school, to ensure all pupils and staff stay safe using artificial intelligence we will pay due regard to government guidance: Generative AI in Schools. For further information on the safe use of Artificial Intelligence, please see linked policy – AI Policy.

Children may also be exposed to risks from AI-generated content, including manipulated or synthetic images, audio and video (often referred to as "deepfakes"), impersonation, misinformation, disinformation, non-consensual image creation and sharing, online grooming and cyberbullying. Staff will respond to concerns involving AI-generated content in line with the Safeguarding and Child Protection Policy and Behaviour Policy.
Ongoing and regular online safeguarding training for staff and pupils will ensure that knowledge is kept up to date in all areas of risk to prevent harm.

The school recognises that AI-enabled wearable devices, including smart glasses, may present safeguarding and privacy risks and will be managed in accordance with this policy.

Filtering and Monitoring:

The Governing Body is committed to taking all reasonable steps to minimise pupils' exposure to the online risks outlined within this policy. The school maintains appropriate filtering and monitoring systems to help provide a safe and secure online environment for all pupils. Beachborough currently uses SENSO and Smoothwall to support its filtering and monitoring arrangements.

Pupils are not permitted to bring mobile devices into school unless specific permission has been granted by the Deputy Head Pastoral and the Head of Learning Success to support a recognised learning, SEN or disability need. Pupils do not have access to the school's Wi-Fi network, except where authorised for educational purposes.

In fulfilling its statutory safeguarding responsibilities, including those under the Prevent Duty, the school has undertaken an appropriate filtering and monitoring risk assessment and has regard to guidance provided by the UK Safer Internet Centre. The Governing Body recognises the importance of ensuring that filtering systems remain proportionate and do not unnecessarily restrict access to legitimate educational resources.

The Deputy Head Pastoral (DSL) has strategic oversight of the school's filtering and monitoring arrangements and works closely with the IT Manager to ensure that systems remain effective, appropriate and responsive to emerging safeguarding risks. Online safety, filtering and monitoring arrangements are reviewed regularly through meetings between the DSL and IT Manager.

In addition, the effectiveness of the school's filtering and monitoring systems is formally reviewed and documented at least annually. Records of these reviews, including any findings, actions and subsequent improvements, are retained by the school. Reviews take account of emerging technologies and evolving online risks, including artificial intelligence tools, AI-generated content and other developments that may impact pupil safety, with outcomes reported through appropriate governance channels.

Education:

The Computing and PSHE curricula play a key role in developing pupils' knowledge, understanding and resilience, enabling them to navigate the online world safely, responsibly and confidently. Through age-appropriate education, pupils are equipped with the skills to protect themselves and others, make informed decisions and seek support when needed.

Our whole-school approach to online safety empowers all staff to educate, support and safeguard pupils in their use of technology, while ensuring that appropriate procedures are in place to identify, respond to and escalate concerns where necessary.

Online safety education includes teaching pupils about digital footprints, online reputation, misinformation and disinformation, cyber security, privacy and security settings, the responsible use of artificial intelligence, healthy online behaviours, and how to report concerns or access support.

Further information regarding the school's online safety education provision should be directed to the Deputy Heads of Manor House or, for Boardman pupils, the Head of Boardman.

Reporting Internet Safety Concerns:

Any pupil, member of staff or parent with a concern relating to online safety should report it, in the first instance, to the Designated Safeguarding Lead (DSL). The DSL will assess the concern and take any appropriate action in accordance with the school's Safeguarding and Child Protection Policy. This may include referrals to external agencies such as Children's Social Care, the police or ESAS where necessary.

Where a concern does not meet the threshold for safeguarding intervention, it will be referred to the appropriate pastoral team for support, investigation and resolution.

The school uses filtering and monitoring systems to help provide a safe online environment and to meet its statutory safeguarding responsibilities. Access to inappropriate or harmful content is restricted and online activity is monitored to identify potential safeguarding concerns. This includes risks associated with social media platforms, online gaming environments, livestreaming services, messaging applications and emerging technologies where pupils may encounter harmful content, contact, conduct or commercial risks.

The school recognises that many pupils access online platforms and digital technologies outside of school. Pupils are therefore reminded that they are expected to uphold the school's values and standards of behaviour at all times, including when engaging online. Any online activity, whether conducted on or off school premises, which brings the school into disrepute, damages the reputation of members of the school community, or involves bullying, harassment, intimidation, threatening behaviour or the sharing of inappropriate content may be treated as a disciplinary matter and dealt with in accordance with the school's Behaviour Policy.

This includes the posting, sharing or distribution of comments, messages, photographs, videos or other digital content on social media platforms, video-sharing sites, messaging services or similar online services.

Responsibilities:

- Ms SJ Lapper is our Deputy Head Pastoral and Designated Safeguarding Lead (DSL). She has overall responsibility for safeguarding, online safety, filtering and monitoring oversight within the school. Pupils, staff and parents are encouraged to speak to her if they have concerns relating to online safety or safeguarding.

The DSL has strategic oversight of online safety, filtering and monitoring arrangements and works with the IT Manager to ensure systems remain effective, proportionate and responsive to emerging safeguarding risks.

- Mr. Dimmock is our Head of IT; he will require all pupils to understand the Acceptable Usage Policy which they agree to when accessing the computers in the computer suites and also complete and understand the Healthy Digital Technology Contract.
- Mr. C Rodd is our IT manager and any questions regarding our technical provision/infrastructure should be directed to him. He will work in conjunction with the safeguarding team to review the school filtering and monitoring systems in place to safeguard our pupils. The IT Manager supports the annual review of filtering and monitoring arrangements and advises the safeguarding team on emerging technologies, cyber security and online risks.
- Mrs. C. Wood is our Bursar. She is our Data Protection Co-ordinator who will endeavour to ensure that all personal data is processed in compliance with regulatory requirements.

Parent and Pupil Responsibilities:

All parents and pupils are expected to read, understand and complete the Acceptable Use Form.

Manor House Guidelines for Pupils Using the School Network, Email and the Internet – Fill out form.

Boardman Guidelines for Pupils Using the School Network, Email and the Internet – Fill out form

This form is issued to parents at the start of each academic year. Parents are asked to review the Acceptable Use Agreement with their child and sign the declaration to confirm that they have read, understood and agree to the school's expectations regarding the safe and responsible use of technology.
In Computing lessons, pupils will also complete a Healthy Digital Technology Contract, designed to promote positive digital habits and encourage the safe, responsible and balanced use of technology in ways that support their own wellbeing and that of others.
Beachborough operates a phone-free environment for pupils. Mobile phones must not be brought into school unless exceptional permission has been granted by the Deputy Head Pastoral and the Head of Learning Success. Where such permission has been given, the device must be handed in to Reception on arrival and collected at the end of the school day.
Pupils are also not permitted to wear or bring smart watches, Meta Smart Glasses, AI-enabled glasses or any other wearable technology capable of recording, storing, transmitting or livestreaming images, audio or video, unless specifically authorised by the school. These devices may present safeguarding, privacy and data protection risks and are therefore prohibited.

Prevent Duty:

- The school delivers a proportionate response with respect to a duty to prevent pupils becoming extremist or radicalised.
- It is recognised that both encouraging extremism and radicalism is a form of child abuse and all staff must treat suspicions as they would any other form of child abuse.
- Evidence suggests that social media is the greatest method used by those who wish to encourage extremism and radicalism.
- The school recognises that extremist content, conspiracy theories, misinformation and disinformation may be encountered through social media platforms, online communities, gaming platforms, video-sharing services and AI-generated content. Staff remain vigilant to these risks and will report concerns in accordance with safeguarding procedures.
- Additional guidance can be found here: www.saferinternet.org.uk www.thinkuknow.co.uk

This policy applies across the whole school including Boarding and EYFS and will be reviewed and updated regularly. ***Linked Policies and read in conjunction with:*** *Safeguarding and Child Protection, Behaviour, Taking and*

Use of images, Social Media, Anti-bullying, Equal Opportunities, Boarding, AI Policy, Staff Code of Conduct and Data Protection.