Beech Hill Primary School

e-Safety Policy 2025-26

To be revised November 2026

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Anti-Bullying, Curriculum, Data Protection and Security.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Newcastle LA Network including the effective management of Websense filtering.
- The school also now has a Cyber Attack response plan in the event of an incident which compromises our IT security.

School e-safety policy

Writing and reviewing the e-safety policy

The e-Safety Policy relates to the school's safeguarding policies and practices as well as to other policies including those for ICT, Anti-Bullying, Child Protection and the DfE's Teaching online safety in schools document (2023).

- The Designated Safeguard Lead has read and agreed that the policy meets the needs of the school, children and staff.
- It has been agreed by all staff and approved by Governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: John Rowlands

Teaching and learning

Why Internet use is important

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- 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 will enhance learning

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

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Newcastle LA.
- 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 on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Publishing pupils' images and work

- Photographs that include pupils and their work will be selected carefully and will adhere to the wishes of parents and carers who do not wish for their children to appear online.

Social networking and personal publishing

- The school, along with help from the LA, will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail address, full names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Computing coordinator and the Designated Safeguard Lead and passed on to the LA.
- The LA will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Staff can raise concerns about an unfiltered website and request it be blocked by the LA.
- Staff can also request a website be unblocked if it is deemed safe for children and is of educational benefit.
- The computing lead will test filtering once a year with the assist of a member of the local advisory board (school governor).

Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed.
- Pupils are not allowed mobile phones in class. If they bring a mobile phone to school, it must be handed to staff at registration for safe keeping, stored securely in the school office and returned at the end of the day.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. "The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently."

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- During periods of school closure such as lockdown, children who require devices can borrow them to assist with home learning.
- Parents will be asked to sign and return a consent form before devices are sent home to pupils.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Newcastle LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will review ICT provision annually to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the management team.
- Any complaint about staff misuse must be referred to the Executive Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be reinforced in all class rooms and the ICT suite and discussed with the pupils.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will have access to the School e-Safety Policy and its understand its importance.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- A range of material will be available on the school website to encourage parental support and offer them guidance

Sexting

Explicit Content on Mobile Phones

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages. A young person is breaking the law if they: take an explicit photo or video of themselves or a friend; share an explicit image or video of a child, even if it's shared between children of the same age; possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

The child will become vulnerable if these photographs are shared publicly and they may become subject to blackmail, bullying or it may cause unwanted attention or emotional distress.

The pupils at Beech Hill Primary School are taught about keeping themselves safe online during Internet Safety Week. Within this time, the children are taught about sending appropriate texts, tweets and other social media messages. They are also taught about the positives of text messaging and the virtual world. As well as the positives, the teachers help the pupils to explore the negatives of using mobile phones and other devices. Additionally, the children in our school learn the risks of sending unwanted or explicit content.

Our children are taught about having a positive self-image and to respect their own bodies throughout school.

Key recent developments in e-safety

Increased Cybersecurity Threats in Schools
Cyberattacks targeting schools, such as phishing and ransomware, have been on the rise, impacting students' education and financial resources. Schools are now encouraged to implement robust cybersecurity measures, such as multi-factor authentication, regular software updates, and cyber incident response plans. These steps can help prevent data breaches and ensure a rapid response in the event of an attack. A Valour Cyber Attack Response Plan has been written to address this.

Generative AI Tools
The rise of generative AI tools like ChatGPT has prompted discussions about their potential misuse, such as generating fake assignments or facilitating cheating. While we aim to embrace aspects of this technology, schools should guide students on ethical AI use and educate staff on identifying AI-generated content. This aligns with building digital literacy skills.

Media Literacy and Misinformation Awareness
A growing concern about misinformation online has led to the inclusion of media literacy education. Students and staff are taught how to evaluate the reliability of online sources and recognise manipulative or false information. For example in Year 4, children are taught to recognise plagiarism, Year 5 are taught to recognise spam and phishing.

Remote Learning and E-Safety Challenges
With the increased use of remote learning tools, safeguarding against privacy breaches during online classes remains critical. Schools are encouraged to use secure platforms and establish clear guidelines for virtual learning to protect student and staff data.

Dame Nicola Stephenson ***Mrs Jess Eatock***
Executive Head Teacher ***Head Teacher***

November 2025