Online Safety Policy

This policy was approved

March 2026

This policy should be reviewed annually

"Together unlocking the potential of every child; inspiring children and changing lives"

Introduction

It is Government policy to connect all schools to the Internet. The internet is a vital educational resource for schools, pupils and teachers. Home internet, mobile phone and email use is widespread, and an important part of learning and communication during leisure time.

However, the internet is managed by a worldwide collaboration of independent agencies. Without appropriate measures, access to unsuitable materials is possible and security of computer systems could be compromised.

This Online Safety Policy has been agreed to ensure that Internet and email use supports the school's educational aims and that the school's responsibilities to students and parents are met.

This Online Safety Policy is included as part of the school's

- Computing Policy.

This Online Safety Policy relates to other school policies, in particular

- Behaviour
- Safeguarding
- Remote Learning
- Social Media policy
- Use of Mobile Phones and Smart Devices in School
- AI Acceptable Use Statement

This Online Safety Policy is written in conjunction with the following agreed school documents:

- Staff, Governor and Volunteer ICT Acceptable Use Agreement
- Be SMART on the Internet

This Online Safety Policy has been ratified following consultation with staff and governors, and will be reviewed on a yearly basis.

The school uses systems for monitoring and filtering pupil and staff usage. Reports from this system are sent to the Designated Safeguarding Lead and are followed up appropriately.

Aims of School Internet and Email access

School internet and email access should be used by staff in order to:

- Raise educational standards
- Support curriculum development in all subjects
- Support staff professional development
- Enhance communication and the exchange of data between schools, the Local Authority and government departments.
- Enhance professional communication and administration within school.

School internet access should be used by pupils where:

- Internet access is planned to enrich and extend learning activities as an integrated aspect of the curriculum
- Pupils are given clear learning objectives for Internet use
- Pupils are provided relevant and suitable web sites and resources
- Pupils will be made aware that the author of a web page, email or text message may not be the person they claim to be, and that information they find online may not be accurate. They are are taught to validate information before accepting it as true.
- Pupils are taught to observe copyright when copying materials from the web and to acknowledge their sources of information
- Pupils are taught to expect a wider range of content than is found in other media sources

Acceptable Use of Internet, Email and use of mobile devices

Staff should use the internet and email only as a tool to support teaching, learning, administration, professional communication and professional development (see above). All staff, governors and volunteers should sign and adhere to the Staff, Governor and Volunteer ICT Acceptable Use Agreement and adhere to the school policy for the Use of Mobile Phones and Smart Devices in School and the and AI Acceptable Use Statement.

Internet access for pupils is an essential part of the school's ICT curriculum and policy. Pupils' access to the internet and email should only be authorised by staff on the basis of educational need.

Staff are responsible for ensuring pupils are using ICT only for school purposes, for educating children on acceptable and safe use of ICT, and for providing appropriate, age related, restrictions, supervision and direction. Staff are responsible for the pupils' safe use of ICT in school.

Use of Learning Platforms

Any use of learning platforms for virtual lessons or homework must adhere to safeguarding protocols and practices. This would include, but is not exclusive to; taking photos of screens, pupils and staff being in a secure environment, log on details not being shared and parents and staff regularly reviewing accounts and usage. When using these platforms, communication by staff, pupils and parents must remain work related and respectful.

Social Networking Websites

Staff are expected to apply the ICT Acceptable Use Agreement and AI Acceptable Use Statement when using social networking websites at any time.

Staff should not communicate with pupils in the school through social networking websites.

Staff should teach pupils to adhere to the age restrictions of social networking websites, e.g. Facebook/ Whatsapp/ Snapchat/ TikTok should not be used by anyone under the age of 13.

Photography and Videos

Staff, governors and volunteers should only use the school's cameras and ICT equipment to photograph pupils during the school day or at school events.

Pupils' photographs and videos should only be submitted for public use, e.g. website, newspapers, if parents have given written consent through our school's Pupil Permissions Form or via email.

Parents should be advised that photographs and videos, including images of other pupils at school events, e.g. plays, sports' day, should not be put into the public domain, e.g. social networking websites.

Online Safety Education

Children are taught online safety across the school through assemblies, 'safer internet days', PSHE, posters, and ICT lesson through Childnet International's Be SMART on the Internet guidance. The SMART guidance for children is as follows:

Safe: Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

Meeting: Meeting someone you have been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

Accepting: Accepting emails, messages, or opening files, pictures or texts from people you don't know or trust can lead to problems- They may contain viruses or nasty messages.

Reliable: Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or you or someone you know is being bullied online.

Cyber- Bullying

"The rapid development of, and widespread access to, technology has provided a new medium for 'virtual bullying', which can occur in and outside school. Cyber-bullying is a different form of bullying which can happen beyond the school day into home and private space, with a potentially bigger audience, and more accessories as people forward on content. Preventing and raising awareness of bullying is essential to keeping incidents in our school to a minimum. Through assemblies as well as PSHE lessons, children are given regular opportunities to discuss what bullying is, as well as incidents we would not describe as bullying, such as two friends falling out, or a one-off argument. Children are taught to tell an adult in school if they are concerned that someone is being bullied." –Beaupré Community Primary School Anti-Bullying Policy

The headteacher or senior member of staff will take action, in accordance with the Anti-Bullying Policy, in response to any allegations of cyber bullying involving pupils, including through the use of text messages and social media, either during or outside of school hours.

Staff should be vigilant in looking out for signs of bullying or other child protection issues (ref. Anti-Bullying Policy).