Policy 7H - E-safety Policy
Including EYFS

(Review annually)

Date	Reviewed by	Date Reviewed by SMT	Date approved Sub-committee	Date approved Governors	Next review date
April 2021	Mrs C Goddings	30.4.2021	Category 1 Policy for May 2021 sub-committee meeting	Category 1 Policy for 23rd June 2021 Court meeting	May 2022 for June 2022 Bridewell Court Meeting
April 2022	Mrs C Goddings	29.04.2022	Category 1 Policy for May 2022 sub-committee meeting		May 2023 for June 2023 Bridewell Court Meeting

Policy Aims

The E-safety Policy is part of The School Development Plan and relates to other policies including those for anti-bullying and cyber bullying (A8) and for child protection (A6).

- The E-safety committee key members are the E-safety Co-ordinator, The School's Designated Safeguarding Lead (DSL) and the Safeguarding Governor.
- The E-safety Coordinator is Mrs C Goddings.
- Our E-safety Policy has been written by the School, building on best practice and Government guidance.
- The E-safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide students 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 Internet will increasingly be used to support children's learning, allowing quick and easy access to research material (often in the form of images and film footage as well as text), online testing resources and providing a platform for shared learning. Teachers may use internet resources to support teaching and learning in class; children may have directed, supervised internet access in lessons and when appropriate may be asked to access the internet as part of research homework.
- The School internet access is provided by Elmbrook Computers Ltd through a fibre broadband connection, which includes filtering appropriate to the age of the children.
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Children will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children will be shown how to publish and present information appropriately to a wider audience.

Children will be taught how to evaluate internet content

- The School will seek to ensure that the use of internet derived materials by staff and by children complies with copyright law.
- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children will be taught to report unpleasant internet content to an adult. For children whose parents lack economic or cultural educational resources, the School should build digital skills and resilience acknowledging the lack of experience and internet at home e.g. ability to complete homework in late study at school.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed annually.

- Virus protection will be updated annually or as required if earlier.
- Security strategies will be discussed with Elmbrook Computers Ltd.
- Any security issues will be directed to Elmbrook by IT Support.

E-mail

- Children and staff may only use approved e-mail accounts on the School system. Staff may access personal email accounts during break times when not on duty or in the presence of children.
- Children must immediately tell a staff member/adult if they receive an offensive e-mail.
- Children must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to children email communication must only take place via a school email address or from within the management information system and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The School does not allow e-mail to or from children and external bodies. The forwarding of chain letters is not permitted.

Mobile Phones and other electronic devices

- The School does not allow the use of personal mobile phones, other electronic devices, music players e.g. iPods, and handheld electronic games in school by children unless the Head has given specific permission. Any child who has to bring a phone to school should hand it in at the School Office and can collect it at the end of the School day. If a child is found in possession of an unauthorised personal device, it will be confiscated and passed to the Head of Organisation and Communication who will lock it in the School's safe. A parent or legal guardian will have to request its return. Where there are safeguarding concerns, a member of staff reserves the right to ask children to unlock their device and search the contents.

Published content and The School website

- The contact details on the Website should be the School's address, email and telephone number. Staff or children's personal information will not be published.
- The Head or Head of Marketing will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing children's' images and work

- Please refer to the School's Use of Images policy (U).

Social networking and personal publishing on The School learning platform

- The School will control access to social networking sites, and consider how to educate children in their safe use e.g. use of passwords. This control may not mean blocking every site, it may mean monitoring and educating children in their use.
- Children will be advised never to give out personal details of any kind which may identify them or their location.
- Children must not place personal photos on any social network space.
- Children and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary and secondary aged children.
- Children will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The School will work in partnership with Elmbrook Computers Ltd to ensure systems to protect children are reviewed and improved.
- If staff or children come across unsuitable on-line materials, the site must be reported to the Head of Organisation and Communication.
- The IT Department will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the Barrow Hills fibre broadband network to ensure quality of service and security.
- Children should ask permission from the supervising teacher before videoconferencing.
- Videoconferencing will be appropriately supervised for the child's age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time, unless under controlled circumstances. The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the School.
- Should contact with children be required, staff will use a school email address.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the School.

Protecting personal data

- Please refer to the School's Data Protection Policy.

Policy Decisions

Authorising internet access

- All staff must read and sign this policy before using any school ICT resource.
- The School will maintain a current record of all staff and children who are granted access to school ICT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Prep Department children will be granted internet access via a School supplied device, and agree to comply with the Acceptable Use of ICT Appendix B (AUP) including Responsible Internet Use Statement.
- Parents will be asked to sign and return a consent form – Appendix B.
- Any person not directly employed by the School will be asked to sign an "Acceptable Use of ICT (AUP)" – Appendix C, before being allowed to access the internet from The School site.

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. Barrow Hills School cannot accept liability for the material accessed, or any consequences of internet access.
- The School will monitor ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.

Handling E-safety complaints

- Complaints of internet misuse will be dealt with by the Director of Organisation and Communication.
- Any complaint about staff misuse must be referred to the Head.
- Complaints of a child protection nature must be dealt with in accordance with School's child protection procedures.
- Children and parents will be informed of the complaints procedure.
- Children and parents will be informed of consequences and sanctions for children misusing the internet and this will be in line with the School's behaviour policy (A4).

Community use of the internet

- All use of the School internet connection by community and other organisations shall be in accordance with the School's E-safety Policy.

Communications Policy

Introducing the E-safety Policy to children

- Appropriate elements of the E-safety Policy will be shared with children.
- E-safety rules will be posted in all classrooms.
- Children will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of E-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.

Staff and the E-safety Policy

- All staff will be given The School E-safety Policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the E-safety Policy and agree to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- The School will ask all new parents to sign the Acceptable Use of ICT Agreement when they accept a place for their child at The School.