Hope Brook C of E Primary School

E-Safety Policy

Learning together and growing together!

Our God given ethos inspires our atmosphere to nurture, raise aspirations and promote life in its fullness. It gives us the breath to develop respectful, enquiring minds, a spirit of curiosity and resilience.
We celebrate the preciousness of each person but water the goodness of working together to bring light into our community.

Light shining on the wider world, radiating HOPE.
Hope and respect for the future
Opportunities for all
Positive relationships that make a difference
Empowering all with knowledge and wisdom

Hope Brook Primary School E-Safety Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school

The IT Co-ordinator is responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy
- That users may only access the school's networks through a properly enforced password protection policy
- That appropriate procedures are followed if any apparent or actual misuse appears to involve illegal activity (Following SWGfL guidance http://www.swgfl.org.uk/safety/default.asp)

Teaching and support staff (including Breakfast Club and After School Club staff) are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy
- E-safety messages are continually reinforced
- Personal data remains 'safe', minimising the risk of its loss or misuse
- They report any suspected misuse or problem to the IT Co-ordinator
- Digital communications with pupils remain on a professional level

Pupils are responsible for:

- Using the school IT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to sign before being given access to school systems
- Using the school IT systems responsibly
- Reporting any misuse of equipment or resources to their classteacher

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school takes every opportunity to help parents understand these issues, particularly through the school newsletter and through the school website.

Parents / carers are responsible for endorsing (by signature) the Pupil Acceptable Usage Policy at the start of each academic year.

Internet Access

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 pupils.

The school Internet access is designed expressly for pupil use and includes 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 safe Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Safeguarding

Our policy complies with the requirements of Keeping Children Safe in Education 2022 . As a school, we raise awareness of how to manage the various types of abuse that can happen on the internet, such as through social networks, text messages and messaging apps, emails and private messaging facilities, online chats, comments on live streaming sites and voice chats in games. A list of helpful links has been

attached to this policy, providing advice and guidance for schools and parents about a range of issues related to internet safety.

Managing Internet Access

Information system security

School IT systems capacity and security are reviewed regularly with our service provider.

Virus and malware protection is updated regularly.

Advice on security strategies are monitored and discussed with our service provider.

Administrator passwords and admin passwords are secure and only accessible to necessary personnel

E-mail

Pupils may only use approved e-mail accounts on the school system and email usage is supervised and monitored by a staff member.

Pupils must immediately tell a teacher if they receive an offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully.

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

Parents / carers are required to indicate whether they allow their children's photographs / work to be displayed on the school website. This permission slip is completed by parents at the start of each academic year (in September).

Pupil's work can only be published with the permission of the pupil and parents.

Pupils work will be saved locally to their tablet or to their personal folder.

Social networking and personal publishing

The school will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved by the IT Coordinator/Headteacher. Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary school aged pupils.

Managing filtering

The school works with the LA, DfE, SWGFL 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 IT Coordinator.

The IT Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies i.e kindles, tablets will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used during lessons or directed school time, except when staff are participating in a school trip.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which includes the principles of General Data Protection Regulation (GDPR) following the principles outlined in our Data Protection Policy

Authorising Internet access

All staff must read and sign the 'Staff Acceptable Use of IT Policy Agreement' before using any school IT resource. (See attached agreement)

All pupils will be asked to sign the 'Acceptable us of IT Equipment E-Safety Rules' agreement. (See attached agreement)

All parents will be asked to sign and return the internet consent form, which refers to responsible use of the internet and includes our 'Rules for responsible internet use'. (See attached agreements)

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

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 GCC can accept liability for the material accessed, or any consequences of Internet access.

The school will audit IT provision 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 senior member of staff and noted on the incidents of misuse form.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Communicating E-safety messages

Staff are responsible for regularly reminding pupils about safe use of IT equipment and monitoring this.

Each year group/class covers E-safety as part of its computing curriculum.

Introducing the E-safety policy to pupils

E-safety rules will be discussed with children at the beginning of the year and at regular intervals throughout the academic year.

Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

All staff will be given the School E-Safety Policy and its importance explained.

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

Parents' attention will be drawn to the School E-Safety Policy through the annual home/school consent packs, the newsletter and through the school web site.

Additional information to accompany this policy:

- **Acceptable Use of IT equipment – E-safety rules KS1 (pupils)**
- **Acceptable Use of IT equipment – E-safety rules KS2 (pupils)**
- **Staff acceptable use of IT Policy agreement**
- **Parent information sheet – Responsible Use of Internet (sent to parents every September with the Autumn Term documents)**
- **A list of useful website links relating to internet safety**

Date of policy: September 2022

Date of next review: September 2023

This policy was formulated in consultation with the Headteacher and teaching staff.

This policy was accepted by the Governing Body at their meeting on Wednesday 12th October 2022, and will be reviewed annually.

A signed copy of this policies can be found in the Hope Brook Policy Folder, stored in the staffroom.