Hope Brook Church of England Primary School

E-Safety Policy

The staff and governors are committed to the development of each child in a positive, healthy and respectful learning environment to encourage all children to achieve their fullest potential.

We want all the children and adults to achieve success through their own efforts, teamwork, self-discipline and motivation; and through links with the Church, the local community and the global community, work towards a better future for themselves and the world in which they live.

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 ICT Co-ordinator is responsible for ensuring:

- That the school's ICT 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 ICT Co-ordinator
- Digital communications with pupils should be on a professional level

Pupils are responsible for:

- Using the school ICT 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 ICT 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.

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 Annex C of Keeping Children Safe in Education 2018 (Copy attached).

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly with our service provider.

Virus and malware protection is updated regularly.

Advice on security strategies will be 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 will be supervised and monitored by a staff member.

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

Where possible, pupils work will be saved locally to their tablet or to their folder on the server.

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 ICT 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 ICT Coordinator.

ICT 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).

Authorising Internet access

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

All pupils will be asked to sign the 'Acceptable us of ICT 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 ICT 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. (See attached forms)

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 ICT equipment and monitoring this.

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.

Date of policy: September 2018

Date of next review: September 2019

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 26th September 2018, and will be reviewed annually.

Signed Jon P Cosh .... Signed S.Sewem ....

Chair of Governors Headteacher

Annex C: Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 85-87. Resources that could support schools and colleges include:

- UKCCIS has recently published its Education for a connected world framework. Online safety is a whole school and college issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18.
- The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk
- Parent Zone and Google have developed Be Internet Legends a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.

Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.[112] The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring.

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCCIS have recently published Online safety in schools and colleges: Questions for the governing board

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 81) and the requirement

[112] The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions

to ensure children are taught about safeguarding, including online safety (paragraph 85), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning