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 remain 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 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 Annex C of Keeping Children Safe in Education 2020 (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 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-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 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.

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).

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 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. (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 IT 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 2020

Date of next review: September 2021

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 14th October 2020, and will be reviewed annually.

Acceptable use of ICT Equipment

E-Safety Rules

I agree to the following rules when using the school's ICT equipment:

- I will look after the ICT equipment
- I will not tell other people my ICT passwords
- I will only open / delete my own files
- I will make sure that I am responsible, polite and sensible when using ICT equipment
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own details such as name, phone number or home address
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I know that my use of ICT can be checked.
- I know that parents / carers will be contacted if a member of school staff is concerned about my e-safety

Staff Acceptable use of ICT

Policy Agreement

I understand that the school ICT system should be used in a responsible way, to ensure that there is no risk to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will remind pupils about the safe use of ICT and will embed e-safety in my work with the pupils.

For my professional and personal safety:

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number or personal email address to pupils
- I will only use the approved secure email system for any school business
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

- I will not install any hardware or software without permission from the ICT co-ordinator
- I will support the school approach to online safety and not deliberately upload or add any images, videos, sounds or text that could upset or offend any member of the school community
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher.
- I understand that all use of internet and related technologies can be monitored and logged and can be made available to the Head teacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- I will support and promote the school's e-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature: _____ Date: _____

Full name: _____(printed)

Job title: _____

Responsible use of the Internet

As part of the pupils' curriculum enhancement and the development of IT skills, Hope Brook Church of England Primary School is providing supervised access to the Internet, including e-mail.

Although there may be concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet.

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will ask permission from a member of staff before using the Internet;
- I will not access other people's files;
- I will use the computers only for school work and homework;
- I will not bring data sticks into school unless I have permission;
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

References for Parents	
Helping parents keep their children safe on line	www.internetmatters.org
Support for parents on a range of issues - From advice on children's mental health to staying safe online	www.nspcc.org.uk
Help and advice for families in a digital world	www.parentinfo.org
The experts in digital family life.	www.parentzone.org.uk

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 88-90. Resources that could support schools and colleges include:

- Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- PSHE association provides guidance to schools on developing their PSHE curriculum

- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources
- UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Protecting children

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.[119] 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, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

---

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

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. UKCIS has published Online safety in schools and colleges: Questions for the governing board to help responsible bodies assure themselves that their online safety arraignments are effective.

Education at home

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges-and-other-providers and safeguarding-and-remote-education

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), 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/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- 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
- UK Council for Internet Safety have provided advice on sexting-in-schools-and-colleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online