Haresfield School internet safety policy

'Trusting in God, together we live, learn and grow.'

OUR SCHOOL VISION

At Haresfield Church of England Primary School we want everyone to know that they are unique, special and worthy in the sight of God and to "Aim High". To be the very best that they can be.

We strive to achieve this through our Christian values rooted curriculum. By working together to learn what God wants for each of us, we offer an ambitious, creative curriculum in which we help each child to flourish and grow. . We endeavour to provide the children in our care with a passion for learning and to appreciate the wonder of our world. When they leave our school our aim is to ensure they have the key skills ready to cope with life at whatever level they are. The school is supported by an effective partnership with parents and the community.

Aims of this policy

The internet safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an internet safety Coordinator. This may be the Designated Senior Lead for child protection as the roles overlap. It is not a technical role.

- Our internet safety Policy has been written by the school, building on local authority and government guidance. It has been agreed by senior management and approved by governors.

- The internet safety Policy was revised by: Head and staff

- It was approved by the Governors on: Autumn 2022

- The next review date is (at least annually): Autumn 2023

Teaching and learning

Internet safety will be provided for staff at a staff meeting annually to ensure skills are up to date.

Why the 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 pupils 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.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include 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 Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

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

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant internet content e.g. using the Hector Protector safety button.

National Curriculum

From September 2014 schools will be expected to embed internet safety into the new curriculum, specifically the new Computing curriculum.

Key stage 1

- Use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet.

Key stage 2

- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Use technology safely, respectfully and responsibly; know a range of ways to report concerns and inappropriate behaviour

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils may only use approved e-mail accounts on the school system.

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

- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school should consider how e-mail from pupils to external bodies is presented and controlled.

- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office or nominated school e-mail addresses.

- 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 so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children. Consult the office for an up to date list of No Photographs.

- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

- Work can only be published with the permission of the pupil and parents/carers.

- Pupil image file names will not refer to the pupil by name.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

- Although social networking is blocked through the filters the school will monitor and control access to social networking sites, and consider how to educate pupils in their safe use.

- Newsgroups will be blocked unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- School staff will never contact or communicate in any way with children through social networking sites or personal e-mail addresses.

- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work with the Gloucestershire CC, SWGFL and Becta to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the internet safety Coordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Haresfield School internet safety policy

Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies – including mobile and smart technology

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones are not permitted at school. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- The use by pupils of cameras in mobile phones will be kept under review.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

- If available staff will be issued with a school phone where contact with school is required.

- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

- The use of the ipad to capture images and videos will be monitored closely by all staff.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (GDPR).

Policy Decisions
Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

- The school will maintain a current record of all staff and pupils 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.

- Parents will be asked to sign and return a consent form.

- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Haresfield School internet safety policy

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Gloucestershire CC can accept liability for any material accessed, or any consequences of Internet access.

- The school should audit Technology use to establish if the internet safety policy is adequate and that the implementation of the internet safety policy is appropriate and effective.

Handling internet safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the headteacher.

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

- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to internet safety.

Communications Policy

Introducing the internet safety policy to pupils

- internet safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- A programme of training in internet safety will be developed based on the materials from the DCSF, Glos CC and BECTA.

- internet safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the internet safety policy

- All staff will be given the School internet safety Policy and its importance explained. An induction for new staff will be carried out explaining the internet safety policy and other related policies.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

- Staff will always use a child friendly safe search engine when accessing the web with pupils such as Ask Jeeves for kids; Yahooligans; CBBC Search; Kidsclick . (Not Google unless supervised).

Haresfield School internet safety policy

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School internet safety Policy in newsletters, the school brochure and on the school Web site.

- The school will maintain a list of internet safety resources for parents/carers.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Monitoring and Evaluating

This policy will be monitored and evaluated by the Head, Senior Management team and the Governors through the Curriculum Committee.

Date of policy   Sept 2022 reviewed annually

Next review   Sept 2023

Signed   .... (Head)

Other Policies linked to this policy

Child Protection Policy
Anti-Bullying Policy
Racial Equality and cultural Diversity Policy
Confidentiality
Behaviour Policy
Acceptable Use Policy
Internet safety Policy

Haresfield School internet safety policy

Appendix 2: Useful resources for teachers

BBC Stay Safe

www.bbc.co.uk/cbbc/help/safesurfing/

Becta http://schools.becta.org.uk/index.php?section=is

Chat Danger www.chatdanger.com/

Child Exploitation and Online Protection Centre www.ceop.gov.uk/

Childnet www.childnet-int.org

Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen www.digizen.org/

Kent internet safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/internet safety_home.cfm

Kidsmart

www.kidsmart.org.uk/

Gloucestershire Police – internet safety

Think U Know www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Alan MacKensie – internet safety adviser (online safety agazine & updates Ditto

www.esafetyadviser.com

Appendix 3: Useful resources for parents

Care for the family www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute www.fosi.org

Internet Watch Foundation www.iwf.org.uk

Kent leaflet for parents: Children, ICT & internet safety
www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com