

**E SAFETY and ACCEPTABLE USE POLICY**

|  |  |
| --- | --- |
| Date policy approved | October 2012 |
| Date policy reviewed | Autumn 2023 |
| Date for next review | Autumn 2024 |
| Committee responsible | FGB |
| Authorisation | Ryan Brown |

**HANSLOPE PRIMARY SCHOOL**

**1.** **EFFECTIVE PRATICE IN E-SAFETY**

At Hanslope Primary School, we know that E-Safety depends on effective practice in each of the following areas:

* Education for the responsible use of ICT by staff and pupils;
* A comprehensive, agreed and implemented e-Safety Policy;
* Secure, filtered broadband from Silverbug
* A school network that complies with the National Education Network standards and specifications.
* Writing and reviewing the e-safety policy
* The child protection policy reflects that children with special educational needs or disabilities (SEND), or certain medical or physical health conditions can face additional barriers, including cognitive understanding (being unable to understand the difference between fact and fiction in online content and then repeating the content/behaviours in schools or colleges, or the consequences of doing so).

We are deeply committed to Safeguarding & Child Protection. This Policy therefore needs to be read in conjunction with the following:

* Child protection Policy
* Acceptable Use Protocol (see below)
* Behaviour/Anti-Bullying Policy
* Health and Safety Policy
* Policy on Social Networking Sites & Personal Internet Presence for School Staff

Our e-Safety Policy has been written by the school.

**2. TEACHING AND LEARNING**

2.2.1 Why the Internet and digital communications are important

We appreciate that the Internet is an essential element in 21st century life for education, business and social interaction. Hanslope Primary 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.

2.2.2 Internet use will enhance learning

* Hanslope Primary School’s 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. E safety is a core part of the computing curriculum and teachers must ensure that children leave the school able to: “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” NC 2014
* 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 “use technology purposefully to create, organise, store, manipulate and retrieve digital content.” NC 2014

2.2.3 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

**2.3 MANAGING INTERNET ACCESS**

2.3.1 Information system security

* School ICT systems security will be reviewed regularly.
* Virus protection will be updated regularly.
* Security strategies will be discussed with ICT consultants and broadband suppliers

2.3.2 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, to both pupils and staff, 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.
* Staff email addresses are only for school use.

2.3.3 Published content and the school web site

* Staff school emails will be published and should be checked on a regular basis.
* Pupil personal contact information will not be published.
* The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil’s images and work

* The use of individual photographs will be discouraged and the school will not publish the names of children in alongside any such photographs.
* Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs. Names of school council members may be published on the website.
* Permission from parents or carers will be obtained before photographs of pupils are published (this includes in newspapers, on the school websites and social media).
* Pupils work maybe published, parental/carers permission will be sought where appropriate.
* 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.

2.3.5 Social networking and personal publishing

* The school will control access to social networking sites, and educating pupils in their safe use will form part of E-safety teacher.
* Message boards/ forums 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 will not use social networking sites in school.
* Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.3.6 Managing filtering

* The school will work with Silverbug, ASK, CEOP 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 e-Safety Coordinator (Harriet Lovegood).
* Regular checks by our IT support company are made to ensure that the filtering

methods selected are appropriate, effective and reasonable.

2.3.7 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.
* When not in use webcams on teacher laptops should be disabled to prevent malicious use.

2.3.8 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.
* The senior leadership team should note that technologies such as mobile phones with data enabled can bypass school filtering systems and present a new route to undesirable material and communications.
* Pupils mobile phones will not be used at school and must be handed to the school office at the start of the school day.
* Games machines including the Sony Playstation, Microsoft Xbox and others must not be used to access the Internet at school, and must be used in accordance with the AUP.

2.3.9 Protecting personal data

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**2.4 POLICY DECISIONS**

2.4.1 Authorising Internet access

* All staff and Governors 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 following adult demonstrations with directly supervised access to specific, approved on-line materials.
* At Key Stage 2 children will be directed to specific sites, which have been checked by the teacher prior to use.
* All pupils will be introduced to the Acceptable Use Agreement (Think then Click – E- safety Rules) and asked to sign before being granted access to school ICT systems.
* Parents will be asked to sign and return a consent form.
* Any person not directly employed by the school will not have access to the Internet.

2.4.2 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. The school cannot accept liability for any material accessed, or any consequences of Internet access.
* The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.4.3 Handling e-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 (see child protection policy).
* 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.

Misuse and on-line bullying

Children and young people are keen adopters of new technologies, but this can also leave them open to the threat of increased bullying - known as online bullying, e-bullying or cyber-bullying. This form of bullying can be defined as follows:

“The use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others”

Bullying can take the form of:

* Text messaging
* Email
* Chat and Social Networking – this should not be an issue for pupils at our school due to age, however we are aware that this requirement can be inadvertently overlooked by parents, if they fail to read the terms and conditions of use, or their child as signed up without seeking their permission
* Instant Messaging

All reported incidents of IT misuse and cyber-bullying will be dealt with in accordance with our Behaviour/Anti-Bullying Policy. We do not see cyber-bullying as any less serious as non-electronic bullying and our standard policies, strategies and sanctions apply.

2.4.4 Community use of the Internet

* Currently the school does not provide community access to the internet.
* The school will promote community awareness of e-safety through the school website or through the usual methods of parental communication, where appropriate.

**2.5 COMMUNICATIONS POLICY**

2.5.1 Introducing the e-safety policy to pupils

* E-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 lessons in e-Safety will be followed, based on the materials from ‘Project Evolve’ (see ‘Hanslope School E-safety progression’ document.
* E-Safety training will be embedded within the ICT scheme of work.

2.5.2 Staff and the e-Safety policy

* All staff will be given the School e-Safety Policy and its importance explained.
* Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

2.5.3 Enlisting parents’ and carers’ support

* Parents’ and carers’ attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
* The school will maintain a list of e-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.

**Appendix 1: Internet use - Possible teaching and learning activities**

|  |  |  |
| --- | --- | --- |
| **Activities** | **Key e-safety issues** | **Relevant websites** |
| Creating web directories to provide easy access to suitable websites. | Pupils should be supervised.  Pupils should be directed to specific, approved on-line materials. | Web directories e.g.  Ikeep bookmarks  Webquest UK  Kent Learning Zone |
| Using search engines to access information from a range of websites. | Filtering must be active and checked frequently.  Pupils should be supervised.  Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Web quests e.g.  Ask Jeeves for kids  Yahooligans  CBBC Search  Kidsclick |
| Exchanging information with other pupils and asking questions of experts via e-mail or blogs. | Pupils should only use approved e-mail accounts or blogs.  Pupils should never give out personal information.  Consider using systems that provide online moderation e.g. SuperClubs Plus. | SuperClubs Plus  School Net Global |
| Publishing pupils’ work on school and other websites. | Pupils‟ full names and other personal information should be omitted.  Pupils‟ work should only be published on „moderated sites‟ and by the school administrator. | Making the News  SuperClubs Plus  Headline History  Kent Grid for Learning  Cluster Microsites  National Education Network  Gallery |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.  Photographs should not enable individual pupils to be identified.  File names should not refer to the pupil by name.  Staff must ensure that published images do not breach copyright laws. | Making the News  SuperClubs Plus  Learninggrids  Museum sites, etc.  Digital Storytelling  BBC – Primary Art  Cluster Microsites  National Education Network  Gallery |
| Audio and video conferencing to gather information and share pupils‟ work. | Pupils should be supervised. | FlashMeeting  National Archives “On-Line”  Global Leap  JANET Videoconferencing  Advisory Service (JVCS) |

**Appendix 2: Useful resources for teachers and parents**

Child Exploitation and Online Protection Centre

[www.ceop.gov.uk/](http://www.ceop.gov.uk/)

Childnet

[www.childnet-int.org/](http://www.childnet-int.org/)

Cyber Café

<http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx>

Digizen

[www.digizen.org/](http://www.digizen.org/)

Kidsmart

[www.kidsmart.org.uk/](http://www.kidsmart.org.uk/)

Think U Know

[www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/)

Safer Children in the Digital World

[www.dfes.gov.uk/byronreview/](http://www.dfes.gov.uk/byronreview/)

Project Evolve

<https://projectevolve.co.uk/>

**Appendix 3: Useful resources for parents**

Family Online Safe Institute

[www.fosi.org](http://www.fosi.org)

Internet Watch Foundation

[www.iwf.org.uk](http://www.iwf.org.uk)

Internet Safety Zone

[www.internetsafetyzone.com](http://www.internetsafetyzone.com)