Hambleton Primary Academy ONLINE SAFETY POLICY

2018

HAMBLETON
PRIMARY ACADEMY

The Acceptable Use of the Internet and related Technologies

Context

"Harnessing Technology: Transforming learning and children's services" sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." ***DfES, eStrategy 2005***

The Green Paper ***Every Child Matters*** and the provisions of the ***Children Act 2004, Working Together to Safeguard Children*** sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband ;

- A school network that complies with the National Education Network standards and specifications.

1.The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2.Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

3.Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Principal ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the Senior Management Team(SMT).

The SMT ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;

- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year.

4.Teaching and learning

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.

5.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 generally be published. The contact details given online should be the school office or specific school areas eg Senco, ICT.

- The Principal 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.

- 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

- The school will 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 should use only moderated social networking sites.

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

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

Managing filtering

- The school will work with the LA 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 SMT.

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

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 wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- 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.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils.

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.

Learning Platforms

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

6.Protecting personal data

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

7.Policy Decisions

Authorising Internet Access

- All staff must read and sign the Acceptable Use Policy Agreement (AUP) 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.

Assessing risks

- The school will take all reasonable precautions to ensure e Safety. 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, YHGfL, nor the LA can 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.

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 Principal.

- Complaints related to child protection will be dealt with in accordance with school/LA child protection procedures.

- Pupils and parents will be informed of pupils who misuse the Internet.

8.Communications Policy

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 training in e-Safety will be developed, possibly based on the materials from 'Child Exploitation and Online Protection Centre' (CEOP).

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

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.

- 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.

Enlisting parents' and carers' support

- **Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school Prospectus and on the school Web site/Learning Platform.**
- **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.**

9. Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, anti-bullying and for child protection.

Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy. It has been agreed by senior management and approved by governors.

The e-Safety Policy was revised by: Mrs H Wood September 2016

The next review date is: September 2017

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.	Parental consent should be sought. 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 The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. 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.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail Kent Learning Zone Cluster Microsite blogs Woodlands Primary School website
Publishing pupils" work on school and other websites.	Pupil and parental consent should be sought prior to publication. 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
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils" work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives “On-Line” Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Chat Danger
www.chatdanger.com/

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

National Society for the Prevention of Cruelty to Children
www.nspcc.org.uk/

Childnet
www.childnet-int.org/

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

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

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

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

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 4 Glossary of Terms

TERM	DEFINITION
Acceptable Use Policy (AUP)	A policy that a user must agree to abide by in order to gain access to a network or the internet. In the school context, it may also cover how other communication devices, such as mobile or camera phones, can be used on the school, premises.
Blog	A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short or frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain, photos, images, sound, video, archives and related links, and can incorporate comments from visitors.
Chatroom	A place where a user can communicate with people more or less instantaneously by typing messages which then appear on your computer screen, and are transmitted across the internet to be read by everyone else participating in the chat at that time. The conversation continues through the exchange of messages. Chat can either be moderated or un-moderated. In the latter case the conversation will be completely unsupervised. It is very easy to fake an identity when participating in a chat so be especially wary.
Discussion Forum/ Messageboard	A discussion site on the internet, often focusing on a special theme, where people can post messages online using the formats specified by the provider of this service. Some discussion forums require registration. Some forums contain an archive, which you can use to search for a given topic. Some forums are moderated where the administrator of the forum has the right to delete or edit any messages posted. or to ban abusive users.
Email Groups / Mailing List	Email mailing lists on specific topics that users can subscribe to. Once subscribed the user receives all the messages sent to the group and anything the user sends in is similarly distributed. It is mainly used to conduct discussions about the topic of the mailing list.
Filtering	A method used to prevent or block users' access to unsuitable material on the internet.
Firewall	A network security system used to restrict internal and external traffic
Hacking	The process of illegally breaking into someone else's computer system, breaching the computer's security.
Information Literacy / Digital Literacy	The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.
Instant Messaging	A form of live chat. Generally a user joins a service (most popular is MSN) and then whenever they log on to the internet their name will appear in a central register. The user can then be contacted by anyone on the register and added to that person's contact list, although they will, of course, have to agree to accept their call. A user's email address must be known before they can be added to someone's list of contacts. With some of the more popular forms of instant messaging a user can join a club and all members of the club are notified when any other member logs on.
International Mobile Equipment Identity (IMEI)	A unique 15-digit serial number for mobile phones. When a phone is lost or stolen the number can be identified as invalid, so rendering the handset useless. It can be found by keying *#06# on your phone's keypad

Internet Service Provider (ISP)	**A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.**
Newsgroups	**Like an electronic bulletin board where people with common interests can keep in touch and up to date. You post to the newsgroup using a newsreader, a basic newsreader is included in Outlook Express. Newsgroups can also include video and music files for download.**
Parental Control Software	**Programmes that allow parents or other responsible adults to control various aspects of how a particular computer or network might interact with the internet. Some internet service providers offer free parental control software to members.**
Peer-to-Peer (P2P)	**P2P software allows users to search for files (such as music or videos) in specific folders of other users who are connected to the software. And therefore, also allows others to search the user's specified folders. These files are mostly copyrighted material and so illegal to download unless the user already owns a legally purchased copy. P2P networks are also littered with viruses.**
Personal Digital Assistant (PDA)	**A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.**
Podcast	**An audio file which can contain music, speaking or a mixture of the two. Can be made by anyone from large companies like the BBC to non-professional individuals. They can be downloaded and played through iTunes or on an iPod.**
Pop-Up	**A new window that opens on top of the active internet browser window. This window does not usually contain it's own web address, however in some cases it can do. Pop-ups that open without the user's request usually contain advertisements. Pop-up blockers are available as part of most browsers.**
SMS / Text Messaging	**Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages**
Social Networking Sites	**Sites such as myspace or bebo which allow users to create an online profile that others can then search for and ask for permission to add that person to their list of friends. The online profile would usually include a photo, the user's age, gender, hometown and a list of their hobbies/favourite things. The user can also post a blog, music and video on their page. People on the user's friend list are allowed to send messages, leave comments or contact the user through instant messaging services.**
Spam	**Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term SPIM (or spIM), describes receiving spam via instant messaging.**
Spoofing	**Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails, or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammers.**
URL	**An abbreviation for uniform resource locator, another way of saying address.**

Virus	**A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.**
Webcam	**A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.**