Headcorn Primary School

E-Safety and Digital Literacy Policy

This policy will be reviewed every 1 year and at any other time if changes are required to comply with changes in legislation, regulation or national or KCC advice. Any amendments will require the approval of the Head Teacher and ICT Co-ordinator.

Approval Body	Head Teacher & ICT Co-ordinator
Approval Date	January 2017
Date for Review	January 2018 (1 Year)
Signed - ICT Co-ordinator	L Peters
Signed - Head Teacher	S Symonds

Introduction

Headcorn Primary School’s E-Safety and Digital Literacy policy has been written by the ICT co-ordinator, building on the Kent Schools and Settings E-Safety Policy Template and government guidance. It has been discussed and agreed by the teaching staff and pupils, and approved by the Head Teacher.

This policy will be **reviewed regularly** in line with the evolving nature of the internet and internet based technologies.

Why e-safety is important at Headcorn School

In today’s society children and adults interact with technologies such as mobile phones, games consoles, tablets and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction in most cases leads to learning opportunities that are greatly beneficial to all but can place children and adults in danger. This policy is designed to provide guidance.

E-safety or online safety relates to issues involving children and adults and their safe use of the relevant technologies that use the internet both in and outside of the school setting.

The purpose of Internet use at Headcorn Primary School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems.

Internet access is a statutory entitlement for students who show a responsible and mature approach to its use. It is a necessary tool for learning.

Pupils also use the internet and related technologies widely outside of school and need to learn how to evaluate internet information and to take care of their own safety and security.

Headcorn School believes that online safety or “e-Safety” is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

How the Internet benefits education at Headcorn Primary School

Benefits of using the internet in education include:

- Access to world-wide educational resources;
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for both pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Exchange of curriculum and administration data with the LA and DfE.
- Communication with support services, professional associations and colleagues.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data with KCC and DfE

How the internet is used to enhance learning at Headcorn Primary School
At present WiFi access is available in all parts of the school including shared areas, the meeting room, and staffroom and school hall. More traditional wired access is available in the ICT suite and throughout the school via wired access points.

- The school internet access is designed expressly for pupil use and will include filtering appropriate to the age of the user.
- Staff internet filtering differs to that of pupils and is controlled via the Light Speed program, which is installed on the server situated in the ICT suite. This regulates the levels of access that different users are allowed and is monitored by the schools technician.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives on Internet use. (see Key Responsibilities section)
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity. (see Key Responsibilities section)
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The use of internet chat rooms and social networking sites by the children is strictly prohibited in school and these sites are blocked. However the school may use social media as a way in which to communicate with the wider school community through its official social media accounts.
- Staff should ensure that the use of Internet materials complies with copyright law.

How pupils learn to evaluate Internet content
Pupils should be taught to be critically aware of the materials they read on the internet and should be shown how to validate information before accepting its accuracy. This in turn will help them to become a more rounded digital citizen. Headcorn School understands that the internet and information communication technologies are now an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

Children are now required to be digitally literate.

Children's understanding and ability to respond to e-safety issues is fostered through the regular delivery of the schools computing scheme of work.

Children are likely to encounter a range of risks online which can be summarised by the three c's. (Conduct, Contact and Content.) Staff, parents and carers should be aware of the following…

	Commercial	**Aggressive**	**Sexual**	**Values**
Content *(Child as recipient)*	Advertising SPAM Copyright Sponsorship	Violent Content Hateful Content	Pornographic Content Unwelcome Sexual Comments	Bais Racist or Extremist Views Misleading Information Body Image and Self Esteem Distressing or offensive content

Contact *(Child as participant)*	Tracking Harvesting Sharing Personal Information	Being bullied, harassed or stalked	Meeting strangers Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming or extremism
Conduct (*Child as actor)*	Illegal Downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating or uploading inappropriate or illegal content Unhealthy or inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information or advice Encouraging others to take risks Sharing extremist views Plagiarism

Access to the internet is filtered through the Kent Community Network. Any concerns can be directed to the EIS KPSN Help desk should useful websites need to be unfiltered or alternatively offensive websites prohibited (kpsn.helpdesk@kent.gov.uk).

If staff or pupils should discover unsuitable sites, the URL (address) and content must be reported to the Internet service provider, as stated above, and the ICT co-ordinator, for more specific filtering. (See *How complaints about internet misuse will be handled?* section for further information.)

Anti-Radicalisation

The school takes steps to ensure that pupils are not subject to terrorist or extremism when using the internet. Headcorn School endeavours to do this by insuring that appropriate filtering is in place and that there is a ridged reporting system on hand, that is well known to staff should anything of concern appear on the internet.

The school staff are aware of procedures/good practice that they should adopt when using the internet with their classes. These guidelines are highlighted elsewhere in this policy and should lead to a reduced threat of pupils being exposed to material of this nature.

Further guidance on radicalisation can be found in the schools Safeguarding Policy.

How email accounts are managed at Headcorn School.

A joint class email account is distributed to each of the Key Stage 2 Classes. This can also be used for internal communication between classes. External email can only be achieved through a list of trusted recipients. These are monitored by the ICT co-ordinator. (Microsoft Office Outlook)

- Pupils may only use approved email accounts on the school system, not MSN or other such service.
- Pupils must immediately tell a teacher if they receive offensive email.
- Teachers must record any concerns about e-safety using ‘The Blue Form’ which is then to be handed in to a senior member of staff.

- Pupils should not reveal personal details in email communication, such as address or telephone numbers.
- Access to some external email accounts may be blocked.
- Whole-class or group email accounts will be used to safeguard anonymity of individuals.

Communications

When using communications technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore only use the school email service to communicate with others when in school.
- Any digital communication i.e. emails between staff and parents/carers must be professional in tone and content. Personal email or text messages must not be used for these communications.
- Users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Students should be taught about the risks of using personal details in communications through e-safety lessons.

Class Blogs

- The use of a blog is encouraged at the school and each class including the Foundation Stage has a blog which can be accessed via the school website.
- Work posted on the class blog must not contain any personal information pertaining to the pupils.
- Pupils will be taught appropriate ways to respond to work posted on their and other classes blogs, retaining their anonymity and always being respectful.

How digital content will be used in school.

From time to time digital images or video footage may be used of pupils for educational purposes and as evidence. It is considered good practice to:

- Understand that photographs and videos are for official school use only,
- Understand that photographs or videos used are in accordance with the Data Protection Act
- Consider the appropriateness of the photograph,
- Ensure that they have parental consent for the use of the pupils digital image. (Relevant information located in school office at request.)
- That common sense is used pertaining to photographing or recording sporting events and their appropriateness is assessed.

How the school's website content is managed

- The point of contact on the school website is the school address, school office email and telephone number.
- Website photographs that include pupils will be selected carefully.
- Pupils full names will not be used anywhere on the school website, particularly in connection with photographs.

- Children whose photographs are not permitted to be used on the school website are listed in the school office. *(Staff should familiarise themselves with this information.)*
- Personal information should not be posted on the school website and only official school email addresses should be used to identify staff.
- A nominated member of staff will take responsibility for the overall editorial duties of the website, in conjunction with the Head teacher. Between them they will ensure that content is accurate and appropriate.
- The website should comply with the DFE's guidelines for publications.

Emerging Internet applications

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

Mobile Phones (Pupil Use)

- The children's <u>use</u> of mobile phones is not permitted in school.
- Should a child need to bring a mobile phone to school for legitimate reasons there must first be an agreement between the head teacher and parent or carer.
- Mobile phones will be clearly marked with the child's name and class
- The mobile phone will be kept in the school office and will leave with the child at the end of each day.
- If a pupil breaches the school policy, then the device will be confiscated and held in a secure place at the school office until the end of the school day.

Mobile Phones (Staff Use)

- Staff phones must be switched to silent during lessons
- Staff are not permitted to use their personal mobile phone to contact children or their families
- If a pre-existing relationship exists then this must be brought to the attention of the senior management team.
- If staff have an educational reason for allowing a child to use their mobile phone then this must be agreed by the head teacher.

Mobile Phones (Parents and Visitor Use)

- If visitors to the school must use a mobile phone while on site it must be in accordance with the schools acceptable use guidelines (see staff use)
- Use of mobile phones to take photographs or video must be in accordance with Headcorn School's image use policy and at the Head Teachers discretion

Acceptable Internet Use and Key Responsibilities

Key Responsibilities of Pupils and Pupil use of the Internet,

- Rules for Internet use will be posted, where possible, near all computers that have internet access. ("Think then Click" posters are displayed around the school building).
- Pupils will be informed that Internet use will be monitored.
- Instruction in safe and responsible use of the Internet should precede Internet access.

- Pupils should be aware of and contribute to good e-safety practice and policy while in and outside of school
- Pupils should know that they can seek help from a trusted adult if things go wrong.
- Pupils should respect the feelings and rights of others both on and offline
- Regular 'e-safety' should be incorporated into and discussed in IT and Computing lessons.
- KS1 pupil's use of the internet will be mainly by adult demonstration, with occasional, directly supervised access to specific pre-approved online materials.

At a level that is appropriate to their individual age, ability and vulnerabilities,

- Pupils should take responsibility for keeping themselves and others safe online.
- Pupils should be aware of the personal risks when using any particular technology and should behave responsibly and safely to limit those risks.

Key responsibilities of all members of staff

- All staff must accept the terms of the "Responsible Internet Use" statement before using any Internet resource in school.
- All staff including teachers, supply staff, teaching assistants and support staff, will be provided with the School E-safety Policy, and have its importance explained.
- Staff must understand that their access to material on the internet may differ from that of pupils in the school. Therefore children should only use the internet through their own login.
- In addition staff should be vigilant when using the internet in front of the class. Filtering levels are different in order to meet the needs of individual members of the school community.
- Live web searches should not be used in view of the children.
- Staff should embed online safety education in the curriculum wherever possible
- Staff should have an up to date awareness of online safety issues and how they relate to the children in their care.
- Staff should try to model good practice when using new and emerging technologies focusing on the positive learning opportunities rather than the negatives.
- It is the responsibility of staff to maintain a professional level of conduct in their personal use of technology both within and outside of school.

Key Responsibilities of Parents and Carers

- To discuss e-safety with their children and support the schools approaches by reinforcing good online behaviour at home.
- They should try to role model safe and responsible use of new and emerging technologies
- Be aware and identify changes in behaviour that could indicate that their child is at risk from online harm.
- Where needed seek help from the school or other appropriate agencies if their child encounters problems online

Monitoring Internet Security

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection is installed on the server and updated regularly.

- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.

How complaints regarding Internet misuse will be handled

Should the need arise parents and teachers must know how and where to report incidents regarding misuse of the Internet. The facts of the misuse will need to be noted, for example where it took place e.g. at school or outside of school. A minor transgression of the rules can be dealt with by the teacher as part of normal class discipline but must be recorded using the schools recording procedure i.e. 'The Blue Form.'. These forms can be found in the school office above the photocopier.

- Follow the school's complaints procedure (and for staff members to follow the appropriate internal staff procedure).
- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint with regard to staff misuse of the internet must be referred to the Head Teacher.
- Relevant members of staff i.e. the ICT co-ordinator and the DSL must be notified so that any filtering can take place promptly.
- Pupils and parents will be informed of the complaints procedure.
- Internet access will be withdrawn on evidence of misuse.
- All e-safety complaints must be recorded by the school on 'The Blue Form' and must include actions taken.
- The procedure for reporting misuse or suspected problems regarding e-safety will be displayed in the staff room.
- Appropriate and specific e-safety training may be delivered after the incident to promote more responsible use in the future

Responsible Internet Use by Staff

- The use of the internet within school should be primarily for the purposes of enhancing teaching and learning or for administration.
- It is understood that the internet may be used by staff for personal reasons but this should not impact on school work.
- The use of the internet to conduct personal business or personal gain is not permitted.
- Staff are not permitted to use the internet for any illegal activity, although not against the law, this includes access to sites that may be meant for adults 18 years and older.
- Staff should not browse for sites that may include the following: offensive, obscene, inflammatory, violent or dangerous material.
- The downloading of any unlicensed materials such as music, film, television programs or pdf is not permitted

How is staff training on e-safety undertaken at Headcorn School?

- Headcorn staff receives guidance/training on both digital literacy and e-safety matters through a regular program of professional development which has been built into the schools continued professional development cycle.
- The school has access to training materials through the SWGfL Boost program and utilises the 360 degree e-safety self-review tool to monitor its progression.

How e-safety will be introduced to parents and pupils

Headcorn Primary School will give regular time for the instruction of e-safety in its ICT or PHSE lessons.

Assemblies on e-safety will be given annually, although should the need arise these session will take place more regularly.

A parent 'e-safety' forum will be provided on a regular cycle.

Useful e-safety programmes and resources used by Headcorn Primary School may include:

- www.thinkuknow.co.uk
- www.childnet.com
- www.swgfl.org.uk
- www.kidsmart.org.uk
- www.internetmatters.org

E-safety Contacts

- School E-Safety Officer (DSL) – Sarah Symonds, Lee Drury, Amanda Robertson
- School E-Safety Governor – Paul Kish
- E-Safety Officer for Kent – Rebecca Avery, Tel: 03000 415797

All teaching staff are required to sign to the effect they have read and understood the guidance laid down in this policy and will endeavour to uphold its integrity to ensure the safe and responsible use of the internet at Headcorn Primary School.

Appendices

Glossary of Useful Terms

Term	**Definition**
Adware	*Computer programs that display adverts on screen. Often installed without the user knowing.*
Blog	*A personal website or webpage*
Chatting	*Taking part in online chat*
Content Filter	*A way of limiting access to material on the internet*
Cookie	*A small file sent to a web browser that keeps track of personal preferences*
Cyberbullying	*Bullying behaviour that take place through electronic means*
Downloading	*The transmission of a file from one computer to another*
Emoji	*A collection of smileys from Japan often used in messaging*
Facebook	*A social networking website*
Flaming	*Sending an aggressive or offensive message over the internet*
Grooming	*When a stranger tries to start a relationship with a child for unlawful purposes.*
Instagram	*A photo sharing social network*
Malware	*Short for malicious software. Programs that are designed to damage your computer.*
Pharming	*A means by which personal information can be gained from a user without permission.*
Phishing	*A mean by which a scammer can get a user to visit a malicious website*
Poof	*An app that instantly hides other apps from view*
Pop Jam	*A similar site to Instagram but aimed at younger children.*
Sexting	*The sending of explicit or sexualised images via picture message*
SMS	*Short messaging service*
Social Networking	*Sites that allow members to keep in touch with friends and family.*
Spam	*Unsolicited mail or junk mail*
Spyware	*The general term for a program that monitors a user's actions*
Tagging	*Key words or phrases that can link to people or websites.*
Troll	*Internet slang for a user who deliberately posts inflammatory comments.*
3G	*Third Generation*
4G	*Fourth Generation*

What to do if…

If a child in your care discloses something to you, related to the internet and the use of technology, then the same reporting procedures used for incidents offline can and should be followed. (Green and/or Blue Forms)

1. If you are worried about a young person for any reason then it is important to tell someone straight away.
2. Ensure that you are familiar with reporting procedures in your workplace and that confidentiality is not promised to the child in question.
3. Report immediately to the designated person, for example the Child Protection Officer, so that the correct steps are taken from the start.
4. Ensure that the child's own words are used and are not changed in any way.
5. The child or young person in question may want to accompany you when you make your report, to be part of the process.

Grooming or other illegal behavior

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to CEOP, the Child Exploitation Online Protection Centre.

(Taken from Childnet.org)