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 2018
Date for Review	January 2019 (1 Year)
Signed - ICT Co-ordinator	L Peters
Signed - Head Teacher	S Symonds

Policy Contents

Policy Aims

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.

It takes into account the DfE statutory guidance proceedures for e-safety

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

The named Govenor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes. Any issues identified will be incorporated into the school's action planning.

The purpose and scope of Headcorn School's online safety policy…

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 pupils should be empowered to build resilience and suitable strategies to manage and respond to online risk.

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, tablets, mobile phones or games consoles.

Links to other policies and practices,

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying policy
- Headcorn E-safety Charter

- Behaviour and Discipline policy
- Child Protection policy
- Applicable Curriculum policies (Computing, PSHE and RSE)
- Data Security policy

Roles and Responsibilities

The school has appointed *Lee Drury* as Designated Safeguarding Lead to be online safety lead. Headcorn School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

Key Responsibilities of the Senior Management Team (SMT)

- **Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.**
- **Ensure that suitable monitoring and filtering are in place.**
- **Work with technical staff to monitor the safety and security of school systems and network.**
- **Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age appropriate understanding of online safety.**
- **Ensure that there are robust reporting channels and proceedures across the school regarding online safety concerns.**
- **Ensure that appropriate risk assessments are undertaken regarding safe use of technology.**

Key Responsibilities of Designated Safeguarding Leads (DSL)

- Act as a named point of contact on all online safeguarding issues and liase with other members of staff or other agencies as appropriate.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up to date, appropriate online safety training.
- Work with staff to coordinate participation in local and national online safety iniatives including Safer Internet Day.
- Maintain records of any online safety concerns.
- Monitor online safety incidents and identify gaps and trends.
- Report online safety concerns to the SMT and Governing body.
- Work with the leadership team to review and update online safety policies on a regular basis.
- Meet regularly with e-safety governor.

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.
- Regular ‘e-safety’ should be incorporated into and discussed in IT and Computing lessons.

- 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
- To read the school's e-safety charter and discuss its implications with their children.

Key Responsibilities of Pupils and Pupil use of the Internet
(At a level which is appropriate to their age range.)

- 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 adhere to the Headcorn E-safety Charter
- Pupils should respect the feelings and rights of others both on and offline.
- Pupils should know that they can seek help from a trusted adult if things go wrong.
- 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 Responsibilites of technical support staff:

- Provide technical support and perspective to the DSL and leadership teams, especially in the development and implementation of appropriate online safety policies and procedures.

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

Monitoring and Filtering

The school uses educational broadband connectivity and 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).

The school uses LIGHTSPEED which blocks sites which can be catagorised as pornography, racial hatred, extremism, gaming and sites of an illegal nature.

The school works with its partners and filtering services to review filtering policy regularly.

If staff or pupils should discover unsuitable sites, the URL (address) and content must be reported to the Internet service provider, as stated above, the ICT co-ordinator, school technician for more specific filtering. The DSL must also be informed so that the breach can be recorded and escalated as appropriate. (See *How complaints about internet misuse will be handled?* section for further information.)

Dealing with Filtering Breaches

The school has a clear procedure for reporting breaches.

- If pupils discover unsuitable sites they will be required to turn off the monitor that they are using and inform a trusted adult.
- The member of staff will report the concern using a 'Blue Form', recording the URL if necessary, and reporting this to the DCL.
- Parents or Carers will be informed of filtering breaches involving their child.

Any material that the school believes is illegal will be reported immeadiately to the appropriate agencies, such as: CEOP or Kent Police.

Security and Management of Headcorn IT systems.

- Virus protection will be updated regularly.
- Unapproved software will not be downloaded to work devices or from unknown email attchments
- Portable media should not be used without specific permission
- There will be appropriate use of logins and passwords across the network.
- All users are exected to log-off or lock their machine if the system is to be unattended for any length of time.

Passwords

- All staff will have their own unique username and private password to access the school system.
- Staff are required to use strong passwords and to change their password when directed by the network system.
- Staff are expected to login as themselves and not as another user at anytime.

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 pupils 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.
- 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 the school web site 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 be aware of 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 and reducing risk.

Headcorn School recognises that the internet is a constantly changing environment with new apps, devices, websites and materials emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit
- Ensure appropriate filtering and monitoring is in place
- Understand that due to the global and connected nature of the internet realise that it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

All members of the school community are made aware of the schools expectations regarding safe and appropriate behaviour online. This is clearly set out in the Headcorn School E-Safety Charter.

Social Media Personal and Official School Use

Headcorn School uses an official Twitter handle to engage in social media with the wider world community. This twitter account is controlled and monitored by two members of staff and has the following intended outcomes.

Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Headcorn School community
- The term social media may include, but is not limited to, blogs, wiki, social networking sites, forums, bulletin boards; online gaming, apps, video and photo sharing sites, chatrooms and instant messenger.
- All members of Headcorn School community are expected to engage in social media in a positive and responsible manner.
- All members of Headcorn School are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on social media services.
- The use of social media, other than the designated school account, during school hours is not permitted.

Personal use of Social Media by Staff

- Safe and professional behaviour advice for staff is outlined in the Headcorn School E-safety Charter.

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within a school. Further actions may be taken if it is found that they have brought the profession or institution into disrepute.
- All members of staff are advised to safeguard themselves when using social media sites. This may include the following measures:
    - Setting appropriate privacy levels of their personal sites
    - Being aware of location sharing services
    - Opting out of public listings
    - Logging out of accounts when not in use
    - Keeping passwords safe and secure
    - Ensuring that personal views are not represented as those of Headcorn school

Personal use of Social Media by Pupils

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive educational approach via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils use of social media both home and at school , will be dealt with according to existing school policies.
- Concerns will be raised with parents and carers as appropriate
- Pupils will be advised to concider the risks of sharing personal details on social meadia sites.

Mobile Phones (Pupil Use)

- The children's use 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

Monitoring Internet Security and Managing Access

- 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.
- All staff, pupils and visitors will be made aware of the school's e-safety charter before being granted use of the school computer system and IT resources.

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. This can include: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. 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

Concerns about Pupil Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these concerns in line with the schools Child Protection Policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and proceedures.
- The school will inform parents and carers of any incidents or concerns involving their child as and when required.

Staff Misuse of the internet

- Any complaint about staff misuse will be referred to the Headteacher, according to the Whistleblowing Policy
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer.)
- Appropraite action will be taken in accordance with the Behaviour Policy and Code of Conduct.

How will e-safety be introduced to parents and carers to promote awareness and engagement?

Headcorn School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will endeavour to build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- By drawing their attention to the school online safety policy and expectations in newsletters, letters and on the school website.
- By requesting that they read distributed online safety information as part of joining Headcorn School
- Requiring them to read and understand the Headcorn School E-Safety Charter

Useful E-safety Resources

- www.thinkuknow.co.uk
- www.ceop.police.uk
- www.childnet.com
- www.commonsensemedia.co.uk
- www.internetmatters.org
- www.saferinternet.org.uk
-

E-safety Contacts

- School E-Safety Officer (DSL) – Lee Drury lee.drury@headcorn.kent.sch.uk
- School E-Safety Governor – David Gardner
- Education Safeguarding Advisor – Rebecca Avery, Tel: 03000 415797
- E-safety Development Officer – Ashley Assiter, Tel 03000 415797 esafetyofficer@kent.gov.uk

---

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

i) Safer Use of Technology

Classroom Use

Headcorn School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Games consoles and other games based technologies
- Digtal cameras, webcams and video cameras

All school owned devices will be used in accordance of the schools E-safety Charter and with appropriate safety and security measures.

Tablet devices will be installed with a blueprint via the Apple Configuration program, which locks the device down suitably for use by pupils. iPads use LIGHTSPEED filtering to provide safe age appropriate websearches.

Members of staff should always evaluate websites, tools and apps fully before use in the classroom takes place or a recommendation is given for home use.

The school will use appropriate search tools

- Google Safe Search
- CBBC Safe Search

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

Supervision

Supervision for pupils will be age and ability appropriate

Foundation Stage and Key Stage One

- Pupils access to the internet will be by adult demonstration, with occasional supervised access to particular websites which support learning outcomes for pupils age range and ability.

Key Stage 2

- Pupils will use age appropriate search engines and online tools
- Children will be directed by the teacher to online materials and resources which support their learning.

ii) Proceedures for responding to specific online incidents.

Dealing with 'Sexting'

If the school are made aware of an incident involving the creation and distribution of youth produced sexual imagery, the school will:

- Act in accordance with the schools Child Protection Policy
- Immeadiately notify a member of the DSL team
- Store the device securely or if the incident has been taken and shared on the school network or devices school will take steps to block and isolate the image.
- Carry out a risk assessment to the pupils involved and check with relevant agencies
- Inform parents and carers if appropriate
- Make a referral to Specialist Child services or Police if appropriate.
- Provide the necessary safe guards and support for pupil/pupils involved.
- Implement appropriate sanctions in accordance with schools Behaviour policy.
- Review handling of any incidents to ensure the best practice was implemented.

Dealing with Online Child Sexual Abuse and Exploitation

If the school are made aware of incidents involving online child sexual abuse of a child, the school will:

- Act in accordance of the schools Child Protection Policy
- Immeadiately notify a member of the DSL team
- Store any devices involved safely and securely
- Immediately inform Kent Police via 101 or 999 (if child is in immeadiate risk)
- Make a referral to Specialist Child Services
- Provide the necessary safe guards and support for pupil/pupils involved
- Review handling of any incidents to ensure the best practice was implemented.

The school will take action regarding online sexual exploitation regardless of whether the incident took place on/off of the school premises, using school or personal equipment.

- Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the CEOP report button.

Dealing with Radicalisation

The school takes reasonable precautions to ensure that pupils are not subject to terrorist ideology 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 is aware of procedures/good practice that they should adopt when using the internet with their classes. These guidelines are highlighted elsewhere in this policy, also in the schools e-safety charter and should lead to a reduced threat of pupils being exposed to material of this nature.

If the school is concerned that a child or parent/carer may be at risk from radicalisation online the DSL will be informed immediately.

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