

Kent Schools Core e-Safety Policy and Audit 2008

Primary and Special School Core Policy

KCC Children, Families, Health and Education Directorate has approved this core e-Safety Policy, which can be used by primary and special schools as a template to construct their own policies.

KCC Children, Families, Health and Education Directorate with Kent Schools, Child Protection, Kent Safeguarding Children Board, ASK, EIS, SEGfL and Kent Police.



Writing a School e-Safety Policy

The Kent Schools e-Safety Policy Guidance available on Kent Trust Web provides a detailed discussion of e-safety issues and links to further information. It is revised annually and should be read in conjunction with the excellent material from Becta and CEOP.

However the school must still write its own e-Safety Policy in order to make its own decisions on balancing educational benefit with potential risk.

A school's e-Safety Policy must cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school's e-safety policy will operate in conjunction with others including policies for Pupil Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children and Security plus any Home-School Agreement.

The CFHE Core e-Safety Policy

This core e-safety policy provides a basic template for the schools policy and has been approved by the Children, Families, Health and Education Directorate. CFHE considers that the policy elements with a **K** bullet are mandatory in order to protect staff, pupils, the school and KCC.

Round bullet items are optional. They may be added selectively where the school feels that that aspect of e-safety is appropriate. These items are likely to require editing to suit particular school situations.

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 from the Kent Community Network;
- A school network that complies with the National Education Network standards and specifications.

Further Information

Rebecca Avery, e-Safety Officer	esafetyofficer@kent.gov.uk
Kent Community Network Helpdesk	01622 206040
ASK curriculum ICT staff	01622 203800
e-Safety materials and links	www.kenttrustweb.org.uk?esafety
Curriculum e-safety advice	www.kented.org.uk/ngfl/ict/safety.htm

E-Safety Audit – Primary / Special



This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Headteacher.

Has the school an e-Safety Policy that complies with Kent guidance?	Y/N
Date of latest update (at least annual):	
The school e-safety policy was agreed by governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Have e-safety materials from CEOP and Becta been obtained?	Y/N
Do all staff sign a Code of Conduct for ICT on appointment?	Y/N
Are all pupils aware of the School's e-Safety Rules?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. KCN, Regional Broadband Consortium, NEN Network)?	Y/N
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	Y/N

School e-safety policy

- K** The “**K**” bullets provide the minimum coverage for a school e-Safety Policy and will help demonstrate that it is compliant with the CFHE approved policy.
- Round bullet points indicate optional items, which may require editing to suit local requirements. Schools should download the Kent e-Safety Policy Guidance for a more detailed discussion of policy and what it should cover.

2.1 Writing and reviewing the e-safety policy

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

- K** The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by:
- It was approved by the Governors on:
- The next review date is (at least annually):

2.2 Teaching and learning

2.2.1 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.

2.2.3 Internet use will enhance learning

- K** The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- K** 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.

2.2.4 Pupils will be taught how to evaluate Internet content

- K** The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

2.3 Managing Internet Access

2.3.1 Information system security

- K** School ICT systems security will be reviewed regularly.
- K** Virus protection will be updated regularly.
- K** Security strategies will be discussed with the Local Authority.

2.3.2 E-mail

- K** Pupils may only use approved e-mail accounts on the school system.
- K** Pupils must immediately tell a teacher if they receive offensive e-mail.
- K** 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.

2.3.3 Published content and the school web site

- K** Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
 - The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil's images and work

- K** 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.
- K** Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- K** Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- K** 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

2.3.5 Social networking and personal publishing

- K** The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- K** Newsgroups will be blocked unless a specific use is approved.
- K** Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
 - Ideally pupils would use only moderated social networking sites, e.g. SuperClubs Plus
 - 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.

2.3.6 Managing filtering

- K** The school will work with the Kent Community Network, ASK and Becta to ensure systems to protect pupils are reviewed and improved.
- K** If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
 - Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing & webcam use

- K** Videoconferencing should use the educational broadband network to ensure quality of service and security.
- K** Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- K** Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

2.3.8 Managing emerging technologies

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

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

2.3.9 Protecting personal data

- K** 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

- K** All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. (www.kenttrustweb.org.uk?esafety)
- K** The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- K** At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
 - Parents will be asked to sign and return a consent form.
 - Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

2.4.2 Assessing risks

- K** The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor KCC can accept liability for any material accessed, or any consequences of Internet access.
- K** 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

- K** Complaints of Internet misuse will be dealt with by a senior member of staff.
- K** 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. (The Kent e-Safety Policy has a flowchart of responses to an incident of concern.)
 - Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
 - Pupils and parents will be informed of consequences for pupils misusing the Internet.
 - Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.4.4 Community use of the Internet

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

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- K** e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- K** Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- K** A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

2.5.2 Staff and the e-Safety policy

- K** 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.

2.5.3 Enlisting parents' and carers' support

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

Becta

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

Chat Danger

www.chatdanger.com/

Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

Childnet

www.childnet-int.org/

Cyber Café

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

Digizen

www.digizen.org/

Kent e-Safety Policy and Guidance, Posters etc

www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart

www.kidsmart.org.uk/

Kent Police – e-Safety

www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Think U Know

www.thinkuknow.co.uk/

Safer Children in the Digital World

www.dfes.gov.uk/byonreview/

Appendix 3: Useful resources for parents

Care for the family

www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

<http://publications.teachernet.gov.uk>

Family Online Safe Institute

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk

Kent leaflet for parents: Children, ICT & e-Safety

www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre

www.parentscentre.gov.uk

Internet Safety Zone

www.internetsafetyzone.com