

Eridge House

E-SAFETY POLICY

The internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. All schools need a policy to help to ensure responsible use and the safety of pupils.

Our e-safety policy is built on the following three core principles:

Educating young people to be responsible users of ICT

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must also learn how to recognise and avoid these risks for themselves as they grow older – to become “internet wise”. The precise nature of the risks faced by young people will change over time as new technologies, fads and fashions take hold, but there are general principles of safe online behaviour that apply to all sorts of situations, e.g. pupils need to know how to react if they come across inappropriate material and that they should not give out personal information such as their address and telephone number to strangers or publish this on the internet. They should also be educated to critically evaluate the quality of the material they find on the internet. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Guided educational use

Significant educational benefits should result from curriculum ICT use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum ICT use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful ICT use will also reduce the opportunities for activities of dubious worth.

Regulation and control

Internet safety depends on staff, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones.

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and displayed at the point of access will help pupils make responsible decisions.

This document describes strategies to help to ensure responsible and safe use. They are based on developing responsibility, guiding pupils towards educational activities and limiting access, in addition to ensuring all at Eridge House remain vigilant.

Policy due for review: September 2011

Eridge House

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection, Confidentiality and Security.

E-Safety Policy

*Points marked with an **M** are mandatory*

- M** The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on local and government guidance. It has been agreed by senior management and school staff in consultation with parents and carers
- The e-Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is 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

- M** The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- M** 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 taught how to evaluate Internet content

- M** The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

(See Appendix 1: Possible Teaching and Learning Activities)

Eridge House

Managing Internet Access

Information system security

- M** School ICT systems capacity and security will be reviewed regularly.
- M** Virus protection will be updated regularly.

E-mail

- M** Pupils may only use approved e-mail accounts on the school system.
- M** Pupils must immediately tell a teacher if they receive offensive e-mail.
- M** Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted
(see **Appendix 2: Acceptable ICT Use Policy**).

Published content and the school web site

- M** The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- M** Photographs that include pupils will be selected carefully and written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- M** Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- M** The school will block/filter access to social networking sites.
- M** Newsgroups will be blocked unless a specific use is approved.
- M** Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Eridge House

Managing filtering

- M** The school will work with the Local Education Authority, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- M** If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
 - The ICT Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

- M** Video-conferencing, where used, should use the educational broadband network to ensure quality of service and security rather than the Internet.
- M** Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- M** Video-conferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- M** Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
 - Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- M** All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- M** The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- M** At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
 - Pupils in Years 5 and 6 will be able to access on-line materials independently.
 - Parents will be asked to sign and return a consent form.

Eridge House

Assessing risks

- M** The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- M** The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- M** Complaints of Internet misuse will be dealt with by a senior member of staff.
- M** 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.
 - Pupils and parents will be informed of the complaints procedure.
 - Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the e-safety policy to pupils

- M** E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- M** Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- M** All staff will be given the School e-Safety Policy and its importance explained.
 - Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- M** Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

Eridge House

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
Using search engines to access information from a range of websites.	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. <ul style="list-style-type: none"> ▪ Ask Jeeves for kids ▪ Yahoooligans ▪ CBBC Search ▪ Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
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.	Making the News SuperClubs Infomapper Headline History
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.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art

Eridge House

<p>Communicating ideas within chat rooms or online forums.</p>	<p>Only chat rooms dedicated to educational use and that are moderated should be used.</p> <p>Access to other social networking sites should be blocked.</p> <p>Pupils should never give out personal information.</p>	<p>SuperClubs Skype FlashMeeting</p>
<p>Audio and video conferencing to gather information and share pupils' work.</p>	<p>Pupils should be supervised.</p> <p>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.</p>	<p>Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum</p>

Eridge House

E-Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an e-Safety Policy that complies with local and national guidance?	Y/N
Date of latest update:	
The Policy was agreed by SMT on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both students and staff?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	Y/N
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Policy due for review: September 2011