



High Firs Primary School e-Safety Policy

Jan 2017

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.

- 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 the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by all staff.
- The e-Safety Policy and its implementation will be reviewed annually.
- Next review: January 2018

2.2 Teaching and learning

2.2.1 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 students 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

- 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

2.2.4 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Kent.

2.3.2 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.
- 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.

2.3.3 Published content and the school web site

- 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.

2.3.4 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, 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.

2.3.5 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- 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 or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.6 Managing filtering

- The school will work with the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- 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

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

2.3.8 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.

2.3.9 Protecting personal data

- 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

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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.
- Access to the Internet will be with adult supervision with occasional directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form.

2.4.2 Assessing risks

- 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. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

2.4.3 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 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.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

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

2.5.2 Staff and the e-Safety policy

- 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.

2.5.3 Enlisting parents' support

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

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. | <p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be directed to specific, approved on-line materials.</p> | <p>Web directories e.g. keep bookmarks</p> <p>Webquest UK</p> <p>Kent Grid for Learning (Tunbridge Wells Network)</p> |
| Using search engines to access information from a range of websites. | <p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.</p> | <p>Web quests e.g.</p> <ul style="list-style-type: none"> ▪ Ask Jeeves for kids ▪ Yahoo!igans ▪ CBBC Search ▪ Kidsclick |
| Exchanging information with other pupils and asking questions of experts via e-mail. | <p>Pupils should only use approved e-mail accounts.</p> <p>Pupils should never give out personal information.</p> <p>Consider using systems that provide online moderation e.g. SuperClubs.</p> | <p>RM EasyMail</p> <p>SuperClubs PLUS</p> <p>Gold Star Café</p> <p>School Net Global</p> <p>Kids Safe-Mail</p> <p>E-mail a children's author</p> <p>E-mail Museums and Galleries</p> |
| Publishing pupils' work on school and other websites. | <p>Pupil and parental consent should be sought prior to publication.</p> <p>Pupils' full names and other personal information should be omitted.</p> | <p>Making the News</p> <p>SuperClubs</p> <p>Infomapper</p> <p>Headline History</p> <p>Kent Grid for Learning</p> <p>Focus on Film</p> |
| Publishing images including photographs of pupils. | <p>Parental consent for publication of photographs should be sought.</p> <p>Photographs should not enable individual pupils to be identified.</p> <p>File names should not refer to the pupil by name.</p> | <p>Making the News</p> <p>SuperClubs</p> <p>Learninggrids</p> <p>Museum sites, etc.</p> <p>Digital Storytelling</p> <p>BBC Primary Art</p> |
| Communicating ideas within chat rooms or online forums. | <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</p> <p>Skype</p> <p>FlashMeeting</p> |

| | | |
|--|--|--|
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. | Skype FlashMeeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum |
|--|--|--|

SEE ACCEPTABLE INTERNET USE POLICY FOR LETTERS LINKED TO RESPONSIBLE USE.

Appendix 2: Responsible Use of the Internet letter

~~On High Firs Primary School headed paper~~

Date

Dear Parents

Responsible Use of the Internet

~~As part of pupils' curriculum enhancement and the development of ICT skills, High Firs Primary School is providing supervised access to the Internet.~~

~~Pupils are able to exchange electronic mail with partner schools and research information from museums, libraries, news providers and suitable Web sites as part of their programme of learning.~~

~~Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with that possibility. We have purchased our Internet access from an educational supplier that operates a filtering system that restricts access to inappropriate materials. All our screens are in public view and, as stated above, access will be reasonably supervised.~~

~~Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable under any circumstances, for any damages arising from your child's use of the internet facilities.~~

~~Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.~~

Please read the attached 'Rules for Responsible Internet Use' and sign and return the consent form so that your child may use the Internet at school.

Yours sincerely

Mr C Turtle
Headteacher

~~HIGH FIRS PRIMARY SCHOOL~~

~~Responsible Internet Use~~

Please complete, sign and return to class teacher

Pupil: _____ Form: _____

~~Pupil's Agreement~~

I have read and I understand the school 'Rules for Responsible Internet Use'. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: _____ Date: _____

~~Parent's Consent for Internet Access~~

I have read and understood the school 'Rules for Responsible Internet Use' and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Date: _____

Please print name:

Online Safety (e-Safety) Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police:

www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kent e-Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: <http://www.mariecollinsfoundation.org.uk/>

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: <https://360safe.org.uk/>

Online Compass (Self review tool for other settings): <http://www.onlinecompass.org.uk/>

