# Ashby Hill Top Primary School

## E-Safety Policy

**Nov 2016 Policy**

**Review date: July 2018**

**Chair of Governors: Mr R.Brewin**

# Ashby Hill Top Primary School

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Policy has been extensively revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

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

## End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering.
- National Education Network standards and specifications.

## E-Safety Audit

This audit has been carried out by the senior leadership team (SLT) assess whether the basics of e-safety are in place. Schools will also design learning activities that are inherently safe and might include those detailed within Appendix 1.

| | |
|---|---|
| The school has an e-Safety Policy that complies with CFE guidance. | Y |
| | |
| The Policy was agreed by governors on: | Nov 2016 |
| The Policy is available for staff | **Y** |
| And for parents on the Website | **Y** |
| The Designated Child Protection Coordinator is | **Steve Garner,** |
| The e-Safety Coordinator is | **Steve Garner** |
| How is e-Safety training provided? | **CPD at staff meetings** |

| | |
|---|---|
| Is the Think U Know training being used? | **Y** |
| All staff sign an Acceptable ICT Use Agreement on appointment. | **Y** |
| Rules for Responsible Use have been set for students: | **Y** |
| These Rules are displayed in all rooms with computers. | **Y** |
| Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access. | **Y** |
| The school filtering policy has been approved by SLT. | **Y** |
| An ICT security audit has been initiated by SLT, possibly using external expertise. | **N** |
| School personal data is collected, stored and used according to the principles of the Data Protection Act. | **Y** |
| Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT. | **Y** |

# School e-safety policy

.

### 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 (Steve Garner) who is also the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been agreed by senior leadership team and approved by governors.
- The e-Safety Policy and its implementation will be reviewed every two years.
- The e-Safety Policy was revised by: S.Garner
- It was approved by the Governors November 2016

# 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.

#### 2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system and for any business relating to Ashby Hill Top School.
- 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 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 pupil's images and work

- The media Agreement will be adhered to so that photographs that include pupils will be selected carefully and will not include children whose parents or carers haven't given permission for their image to be used.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Twitter feed by way of signed Media Agreement.
- Pupil's work can only be published with the permission of the pupil and parents.

#### 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

- If staff or pupils discover an unsuitable site, it 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

- 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 & Skype will be appropriately supervised for the pupils' age.
- Skype will be managed by the supervising adult who will connect using a protected password.
- Use of video for teaching purposes; i.e.; IRiS – agreement is sought from the parents where media agreements have not been signed or where the material will be made public.

#### 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, visitors, governors and trainees must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all persons 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.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

### 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. Ashby Hill Top School cannot 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 reported to the e-safety coordinator and then passed onto a member of the SLT.
- 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.

### 2.4.4 Community use of the Internet

- The school will liaise with local community as the need arises to establish safe working practice and create a risk assessment to ensure e-safety procedures are followed.

## 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.
- All staff will read and sign the Acceptable agreement Form (see appendix 4)

### 2.5.3 Enlisting parents' support

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

**Appendix 1: Internet use - Possible teaching and learning activities**

| Activities | Key e-safety issues | Relevant websites examples |
|---|---|---|
| Creating web directories to provide easy access to suitable websites. | Pupils should be supervised.<br>Pupils should be directed to specific, approved on-line materials. | Web directories e.g.<br>Ikeep bookmarks<br>Webquest UK |
| Using search engines to access information from a range of websites. | Pupils should be supervised.<br>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.<br>- Ask Jeeves for kids<br>- Yahooligans<br>- CBBC Search<br>- Kidsclick |
| Exchanging information with other pupils and asking questions of experts via e-mail. | Pupils should only use approved e-mail accounts.<br>Pupils should never give out personal information.<br>Consider using systems that provide online moderation e.g. SuperClubs. | E-mail a children's author<br>E-mail Museums and Galleries |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication.<br>Pupils' full names and other personal information should be omitted. | Making the News<br>Saatchi Gallery<br>Infomapper<br>Headline History<br>Kent Grid for Learning<br>Focus on Film<br>Film Club |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.<br>Photographs should not enable individual pupils to be identified.<br>File names should not refer to the pupil by name. | Making the News<br>SuperClubs<br>Learninggrids<br>Museum sites, etc.<br>Digital Storytelling<br>BBC – Primary Art |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br>Pupils should never give out personal information.<br>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. | Skype<br>FlashMeeting<br>National Archives "On-Line"<br>Global Leap<br>National History Museum<br>Imperial War Museum |

Appendix 2

# Ashby Hill Top Primary School

# e-Safety Rules

***All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.***

| | |
|---|---|
| ***Pupil:*** ***(insert name)*** | ***Class:*** ***(insert class)*** |

**Pupil's Agreement**

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

| | |
|---|---|
| ***Signed:*** | ***Date:*** |

**Parent's Consent for Web Publication and Twitter of Work and Photographs**

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

**Parent's Consent for Internet Access**

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the 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:***

Please complete, sign and return to the school

Key Stage 1

# Think then Click

## These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

# Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

Ashby Hill Top Primary School

# Employee, Volunteer, Trainee and Visitor
# Acceptable Use Agreement / Code of Conduct for E Safety

**ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an excepted part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Designated Senior Person for child protection and safeguarding.**

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must password protected.
- I will not install any hardware or software without permission of the head or deputy.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
  Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher. They should not be stored on personal devices such as mobiles or personal cameras. Images should be uploaded to the server and then removed from personal devices before leaving the premises.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the reputation of the school or my professional role into disrepute.

- This includes the use of Facebook and other social media and comments I may write. Writing comments on Facebook during the school day is not acceptable as this reflects badly on the practice of the school. Comments about school and its members are not acceptable on social networks sites, including Facebook.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- To this end, I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the E-Safety Coordinator, the designated Child Protection Officer or Headteacher.
- I understand this forms part of the terms and conditions set out in my contract of employment.

**User Signature**

I understand and agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name …….....(printed)

Job title ……