

## **E-SAFETY POLICY**



**The Directors of the Governing Body of Hadrian Academy Trust have agreed that policy documentation from Hadrian Lower School will continue to be appropriate until such time that the policy is due to be updated.**

Note;

- The wording Hadrian Lower School should be read as Hadrian Academy.
- Reference to the Local Authority may not always apply.
- Reference to staff employer should be read as Hadrian Academy Trust.

**AGREED BY DIRECTORS OF HADRIAN ACADEMY TRUST:**

Renewal date : Summer 2012

The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

The school's Leadership team will also act as E-Safety Coordinators.

Our E-Safety Policy has been written by the school, building on the NYCC E-Safety Policy and government guidance. Children and parents are asked to sign a formal agreement agreeing to abide by the school code of conduct as part of e-safety.

*It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually, each summer term*

## **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 children 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**

The school Internet access is designed expressly for pupil use and includes filtering materials 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.

### **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.

## **Managing Internet Access**

### **Information system security**

School ICT systems capacity and security will be reviewed regularly.

Virus protection is updated regularly.

Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary once the learning platform is launched.

### **E-mail**

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.

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.

## **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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

## **Publishing pupil's images and work**

Photographs that include pupils will be selected carefully and will only be used with parental permission.

Pupils' full names may be used anywhere on the Web site. However, when used in association with photographs every effort will be made to make it hard to identify individuals.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Pupil's work can only be published with the permission of the pupil and parents.

Permission is sought when a child first enters the school and is part of the Home School Agreement.

## **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 that 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.

## **Managing filtering**

The school will work with the LA, DCSF 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.

School technician staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## **Managing video conferencing**

When this becomes available within the school, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

## **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.

Mobile phones are actively discouraged and will not be used during lessons or formal school time.

## **Protecting personal data**

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

## **Policy Decisions**

## **Authorising Internet access**

All staff and pupils will be asked to 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.

For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form, as part of the Home School Agreement.

## **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 NYCC 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.

## **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 head teacher.

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 to establish procedures for handling potentially illegal issues

## **Communications Policy**

### **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.

### **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.

### **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.

This policy is reviewed annually in the summer term.

## Appendix 1

### Section 4 – Pupil Internet Access

#### Rules for Responsible Internet use

- I will only use ICT in school for school purposes.
- I will only use my class email address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- 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 know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

**Pupil's Agreement**

I agree to follow the Rules as set out above for Responsible Internet Use.

Signed ..... (child's signature)

Year 1 and 2 parents should discuss about keeping safe. Children in year 1 and 2 are too young to have a school email account. Children in Year 3 and 4 will have a school email account.

**Parent / Guardian**

I am aware of the guidance above that my child must abide by when using the internet in school.

Signed ..... (parent/guardian)

Date: .....