

# E-Safety Policy for New Christ Church Primary School

November 2009

## **E-Safety**

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 Behaviour, Bullying, Curriculum, Data Protection and Security,

### **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 from Reading Borough Council network including the effective management of Websense filtering.
- National Education Network standards and specifications.

## **SCHOOL e-SAFETY POLICY**

### **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 e-safety co-ordinator is the Headteacher.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by Maria Soulsby

## **TEACHING AND LEARNING**

### **Why Internet use is important**

- The internet is an essential element in 21<sup>st</sup> 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.

### **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.

### **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 systems security**

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

### **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.

### **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.

### **Publishing pupil's 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 website.

### **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.

### **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 co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **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

### **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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden
- No member of staff should use their personal (ie Other than New Christ Church School) e-mail address for contact with pupils, parents or governors on School related matters.
- Staff are to be advised on appropriate personal security measures when using the internet or personal mobile phones.

### **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 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.
- At 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.

### **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. The 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.

### **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.

## **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 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.

Reviewed Nov 2009

Approved by Governors: 8.12.09

To be reviewed December 2010

### 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 VLE
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"> <li>• Ask Jeeves</li> <li>• Yahoo!igans</li> <li>• CBBC Search</li> <li>• Kidsclick</li> </ul>
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 websites other than the school's	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 RBC VLE Focus on Film
Publishing images including photographs of pupils	Parental consent for publication should be sought Photographs should not enable individual pupils to be identified File name should not refer to the pupil by name	Making the News SuperClubs Learninggrids Museum sites etc Digital storytelling BBC – Primary Art
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 Skype FlashMeeting
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 National History Museum Imperial War Museum

## 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

B. Stoneham & J Barrett

## Think then Click

e-Safety Rules for Key Stage 2

We ask permission before using the Internet

We only use websites that an adult has chosen

We tell an adult if we see anything we re uncomfortable with

We immediately close any webpage we are 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

# New Christ Church Primary School

## e-Safety Rules

*All pupils use computer facilities including Internet access as an n 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: \_\_\_\_\_ 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 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 office.

# Staff Information Systems Code of Conduct

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-Safety policy for further information and clarification.**

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner
- I will ensure that my information systems use will always be compatible with my professional role
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance
- I will respect system security and I will not disclose any password or security information to anyone other than appropriate system manager
- I will not install any software or hardware without permission
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely
- I will respect copyright and intellectual property rights
- I will report any incidents of concern regarding children's safety to the school e-Safety Co-ordinator or the Designated Child Protection Co-ordinator
- I will ensure that any electronic communications with pupils are compatible with my professional role
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed \_\_\_\_\_ Capitals \_\_\_\_\_ Date \_\_\_\_\_

Accepted for School \_\_\_\_\_ Capitals \_\_\_\_\_