



## **E-SAFETY POLICY**

March 2014

## **E-SAFETY POLICY**

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 Policy reflects 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, Anti-Bullying, Curriculum, Data Protection and Security.

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

- Responsible Information and Communication Technology (ICT) use by all staff and pupils; 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 Network including the effective management of Websense filtering.
- National Education Network standards and specifications

### **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

- The school Internet access is designed expressly for pupil use and includes filtering.
- 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 find and they will be 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 will be updated regularly.
- Security strategies will be discussed with Warwickshire County Council (WCC).

### **E-mail**

- Pupils will only use class 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 organization should be written carefully and authorized before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

### **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 has overall editorial responsibility and ensure that content is accurate and appropriate.

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

- It is the policy of the school that when publishing to the school website children's surnames will not be used, nor will any photographs which clearly identify any children.
- If children's photos are necessary written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

### **Social networking and personal publishing**

- Warwickshire County Council will block/filter access to social networking sites on behalf of the school.
- 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 Local Authority (LA), Department of Children, Schools and Families (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.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **Protecting personal data**

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

### **Authorising Internet access**

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All staff and pupils are granted Internet access. Upon leaving access will be withdrawn.
- At Key Stage 1 and Reception, 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.
- Neither the school nor WCC 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**

- A senior member of staff will deal with complaints of Internet misuse.
- 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.

### **Introducing the e-safety policy to pupils**

- E-safety rules will be discussed with the pupils at the start of each year.
- Pupils will be told 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.

### **Failure to Comply**

- Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.

The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.

### **Reviewing the e-safety policy**

The e-Safety Policy and its implementation will be reviewed annually.

REVIEWED    MARCH 2014