Cubbington C E Primary School

E-Safety Policy

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as 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.

Our e-safety policy operates in conjunction with other policies such as those for ICT, Behaviour, Anti- Bullying, Curriculum and Data Protection.

This policy has been strongly influenced by the work of the Kent e-Safety team.

End to End e-Safety

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

- Responsible 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 from the Warwickshire Broadband including the effective management of Websense filtering and Policy Central monitoring.
- National Education Network standards and specifications.

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of our rolling programme for policy development. It relates to other policies such as those for ICT and for child protection.

- The school has appointed an e-Safety Coordinator. This is also the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors.
- The e-Safety Policy will be reviewed annually along with the child protection policy.

1.2 Teaching and learning

1.2.1 Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. We have 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.

1.2.3 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.
- Internet access is used where appropriate to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school e-safety officer.
- We will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 Managing Internet Access

1.3.1 Information system security

The security of the school information systems is maintained through:

- Virus protection being installed and updated regularly.
- Using the Warwickshire Broadband with its firewall and filters.
- Provision of an additional level of protection through deployment of Policy Central in partnership with Warwickshire ICT Development Services. This is a monitoring system with automatic links to the police service.

1.3.2 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.
- Use of words included in the Policy Central ‘banned’ list will be detected and logged.
- Whole-class or group e-mail addresses could be used in primary schools.
- Pupil e-mails 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.

1.3.3 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 without their permission, or that of their parent or guardian.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupil’s images and work

- Pupils’ full names will not be used anywhere on the Web site, particularly in association with photographs.
- Permission from parents or carers will be obtained before identifiable photographs of pupils are published on the school Web site.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Staff are advised to ensure their profiles on social networking sites are set to private and not to add past or present pupils as friends.

1.3.6 Managing filtering

- We will work in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Staff will monitor any occurrence of improper use and put into effect any appropriate changes to the filtering methods selected.

1.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.

1.3.8 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.
- Mobile phones will not be used during lessons. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

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

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the acceptable ICT use agreement, 'E-Safety Agreement Form for School Staff', before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At KS2 pupils will be guided by the Full Rules of Responsible ICT use.

1.4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. We 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 headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.3 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 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.

1.4.4 Community use of the Internet

- We will liaise with external users (e.g. School's Out) to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- There will be planned opportunities to raise the awareness and importance of safe and responsible internet use, both for pupils and parents e.g. CEOPS resources for children, assemblies, cluster workshops for parents.
- Pupil Rules for Responsible ICT use will be revisited annually. At KS1 reference will be made to a simplified version of the Rules of Responsible ICT Use. At KS2 pupils will sign an agreement to abide by the Full Rules of Responsible ICT Use.

1.5.2 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.

1.5.2 Enlisting parents' support

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

1.6 Reviewing this policy

The e-Safety Policy will be reviewed annually in line with the Safeguarding Policy.

Agreed by …………………………..............Date ………………………..

Next Review ………………………………………………………….