



St. Edward's RC Primary School

E-Safety Policy

Created by Mr. P. Phillips (ICTCO) and Mr P. Ward (Headteacher)

Policy Agreed by Governors: February 2018

To be reviewed : March 2019

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and i-pads 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. The school's e-safety operates in conjunction with other policies including those for Student 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 the Warwickshire Broadband including the effective management of BECTA filtering and Policy Central monitoring.
- National Education Network standards and specifications.

1.1 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 and for child protection.

- The school has appointed an e-Safety Coordinator (ICTCO). They will liaise with the Designated Child Protection Coordinator (Head teacher) 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.

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. 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.

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 which Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should 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.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read.

1.3 MANAGING INTERNET ACCESS

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services.

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.
- E-mail sent to an external organisation will 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.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or social media.
- Pupil's work is chosen carefully before publishing eg. If containing personal information

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.
- On school entry a parents' pack will be issued containing safety advice, our school ICT rules and age-appropriate pupil and parent agreement forms. See 1.4.1 for more details.
- The school has a 'Twitter' and 'Flickr' page that can interact and communicate with parents. This account is set to 'private'. Only people who have been accepted by school administrators to the page can view the material. Written permission from parents or carers will be obtained before photographs of pupils are published.

• 1.3.6 Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service and BECTA 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.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing Videoconferencing

- The school will use the Warwickshire Portal using adobe connect for Videoconferencing.

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.
- Pupils should not bring or use mobile phones at school or on school trips, unless previously arranged with the head teacher. 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

- All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use.
- At Key Stage 1 and 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

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. 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 head teacher 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.
- Sanctions within the school discipline policy include:
 - interview/counselling by class teacher or head teacher;
 - informing parents or carers;
 - removal of Internet or computer access for a period.

1.4.4 Community use of the Internet

- 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 and staff will draw pupils attention to this.
- Pupils will be informed that Internet use will be monitored.
- An e-Safety training programme will be taught within lessons across ag groups as part of curriculum and awareness days.

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.

1.5.3 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.

Further Information

Warwickshire ICT Development Service

01926 414100 or www.ictds.org

Sarah Fitzgerald, e-Learning Adviser.

fitzgerald.s1@welearn365.com

Jane Key, Senior e-Learning Adviser.

key.j2@welearn365.com

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. | <p>Pupils should be supervised.</p> <p>Pupils should be directed to specific, approved on-line materials.</p> | <p>Web directories e.g. Ikeep bookmarks Webquest UK Kent Grid for Learning (Tunbridge Wells Network)</p> |
| Using search engines to access information from a range of websites. | <p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.</p> | <p>Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick</p> |
| Exchanging information with other pupils and asking questions of experts via e-mail. | <p>Pupils should only use approved e-mail accounts.</p> <p>Pupils should never give out personal information.</p> <p>Consider using systems that provide online moderation e.g. SuperClubs</p> | <p>RM Easimail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries Welearn365</p> |
| | | |
| Publishing images including photographs of pupils. | <p>Parental consent for publication of photographs should be sought.</p> | <p>Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC - Primary Art</p> |