The Blue Coat CE (Aided) Infant and Junior School's Federation

E-Safety Policy

The following whole school policy refers to the safe, acceptable and responsible use of the internet.

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.

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

- Responsible ICT use by all staff and students
- Sound implementation of e-safety policy in both administration and curriculum.
- Safe and secure broadband including the effective management of filters.
- National Education Network standards and specifications.

School 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.
- Our e-Safety Policy has been agreed by senior management and approved by governors and the PTA.

E-Safety policy

Teaching and learning

Why Internet use is important

- The Internet is an essential element 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 is designed for pupil use and includes 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
- 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 will be updated regularly.
- Security strategies will be reviewed 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.

Published content and the school web site

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the school website particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents.

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 Education Walsall, DCFS 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 named e-Safety person.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

- Mobile phones should not be used during formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

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

ICT access

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Pupils' access to the Internet will be under adult supervision at all times.
- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user
- E-safety rules will be posted in all rooms where there is computer access and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Parents will be asked to sign and return an Internet access consent form.
- 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 Education Walsall can accept liability for the material accessed, or any consequences of Internet access.
- Complaints of Internet misuse will be dealt with by the Head of School.
- SMT undertake an e-Safety audit each year to assess whether the e-safety basics are in place.