Bryn St. Peter's C.E. Primary 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. 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 was revised by L. Pennington. It was approved by the Governors on 10th March 2010. The next review date: March 2011.

Teaching and Learning

Why the Internet and Digital Communications are 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 will be designed expressly for pupil use and will include filtering appropriate to the age of pupils, including RM filters and Securus Software. 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 will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Information System Security

School ICT systems security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with the Local Authority, we use Securus Software on all school systems.

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. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. The forwarding of chain letters is not permitted.

Published content and the school web site

Staff or pupil personal contact information will not be published. The contact details given online should be the school office. Only children's first names will be given other than in exceptional circumstances.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. This will be obtained on an annual basis.

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use. 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, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

The school will work with Wigan Education Authority and Becta to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the ICT coordinator.

Managing Videoconferencing & Webcam use

Video conferencing should use the educational broadband network to ensure quality of service and security. Pupils must ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing and webcam use 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. The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Children are forbidden from bringing technology in from home, except in certain circumstances. The appropriate use of Learning Platforms will be discussed and reviewed. The VLN will be implemented throughout the school in a rolling programme.

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 'Staff Code of Conduct for ICT' before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. Parents and children will be asked to sign and return consent form.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access. The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and 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 (see schools complaints policy) Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community Use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety Policy to Pupils

e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and Internet use will be monitored and appropriately followed up using Securus Software. A programme of training in e-Safety will be developed, possibly based on the materials from CEOP. E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education.

Staff and the e-Safety Policy

All staff will be given the School e-Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting Parents’ and Carers’ Support

Parents’ and carers’ attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site. The school will maintain a list of e-safety resources for parent/carers. The school will ask all new parents to sign the parent/pupils agreement when their child starts school.