Policy for e-Safety

Overview

The school adheres to the Guidelines for Handling the Internet and Electronic Media as set out in the Manual of Personnel Practice. Where necessary the Local Authority guidelines will take precedent.

The computer system is owned by the school and is made available to staff for professional activities and to pupils to further their education and the school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

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.

The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

Our e-Safety Policy has been written by the school, building on the Portsmouth e-Safety Policy and government guidance.

The school's e-safety policy will operate in conjunction with other policies including those for ICT, Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security.

The school has a separate Acceptable Use Agreement for staff.

The e-Safety manager will be the ICT manager.

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.

Pupils may use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

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 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.

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 read and shown how to validate information before accepting its accuracy.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

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 Portsmouth City Council Education Authority.

Access should only be made via the authorised internet service provider, which should not be modified by any person using the internet;

Staff must respect the ICT system security and are reminded that it is a criminal offence to use a computer for a purpose not permitted by the school.

Staff will not disclose any password or login name to anyone, other than where appropriate, to staff responsible for maintaining the system.

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.

The forwarding of chain letters is not permitted.
Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
Staff will ensure that electronic communications with pupils are compatible with their professional role and cannot be misinterpreted
Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received and staff must remain professional at all times

Published content and the school Website

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 ICT Manager 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 Web site or Blog, 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.

Written permission will be sought when the named work of children will be published.

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 are advised when they sign the internet agreement form that the use of social network spaces outside school is inappropriate for primary aged pupils. This information is also displayed in the classroom and staff remind pupils during discussions regarding internet safety.

Use for personal financial gain, advertising, gambling, political purposes, accessing pornographic, racist or offensive material is forbidden;

Staff may make occasional personal use of the internet facilities provided it is in their own time, eg at lunch-time, and provided it does not interfere with the school's work, conforms to the PCC Policy and is not associated with outside business interests.

Managing filtering

The school will work with PCC, DCFS and the Internet Service Providers to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, or have any concerns, it must be reported to the e-Safety Manager or Child Protection Officer if appropriate.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation or Child Protection and Online Protection Centre.

Managing video conferencing

Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils should ask permission from the supervising teacher before making or answering a video conference call.

Video conferencing 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.

Mobile phones will not be used in school by pupils and will be held securely by school staff. Adults are not permitted to use mobile phones in areas of the school where children are present. The sending of abusive or inappropriate text messages is forbidden.

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

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

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 PCC 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.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

The installation of hardware and software cannot be undertaken without the permission of the ICT Manager and staff are reminded of this through this policy and the staff handbook.

Methods to identify, assess and minimise risks will be reviewed regularly.

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.

Parents and pupils will need to work in partnership with staff to resolve issues.

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 shared and displayed in all networked rooms with Internet access. They will be referred to when children are using the internet.
In addition, children in Key Stage 1 will be taught the importance of safe internet use.
Children in Key Stage 2 will receive e-safety lessons in the Autumn term and this will be regularly revisited throughout the course of the year.
Pupils will be informed that network and Internet use will be monitored.

Staff and the e-safety policy

All staff must read this policy which is incorporated within the staff handbook. Staff will be asked to sign for receipt of the handbook and to state that they have read and understood the importance of the Policy for e-safety.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

Internet activity must be compatible with staff professional activity or the student's education;

Enlisting parents' support

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

Parents receive a copy of the school's rules regarding pupils' use of the internet and are requested to give permission for their child to access this facility. Children in KS2 are similarly asked to sign the letter.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Revised November 2012

Review Date July 2015