RUSTINGTON
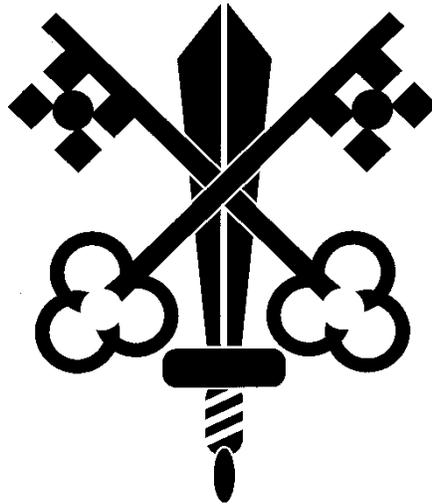
COMMUNITY

PRIMARY

SCHOOL

e-Safety

Date of policy review: February 2014
Next review: February 2015

e-Safety at Rustington Community Primary School

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

The Headteacher has the role of e-Safety Coordinator. The e-Safety Coordinator is also the nominated member of staff responsible for Child Protection. The e-Safety Coordinator is not a technical role.

Our e-Safety Policy has been written by the school, building on Local Authority and government guidance. It has been agreed by senior management and approved by governors.

Teaching and learning

Why the Internet and digital communications are important

- o 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.

- o Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- o Internet access has been designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- o Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- o Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- o Pupils are shown how to publish and present information to a wider audience.

Pupils are taught how to evaluate Internet content

- o Internet derived materials used by staff and pupils should comply with copyright law.

- o Pupils are taught the importance of cross-checking information before accepting its accuracy.

- o Pupils are taught to report unpleasant Internet content to their class teacher who will share this information with the e-safety Co-ordinator.

Managing Internet Access

Information system security

- o School ICT systems security are reviewed regularly.

- o Virus protection is updated regularly.

E-mail

- o Pupils may only use approved e-mail accounts on the school system.

- o Pupils must immediately tell a teacher if they receive offensive e-mail.

- o In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- o Incoming e-mail should be treated with care and attachments not opened unless the author is known.

- o The school does not encourage e-mail from pupils to external bodies unless the contact is well known.

- o The forwarding of chain letters is not permitted.

Published content and the school web site

- o Staff contact information and pupil details are not available on the website.

- o The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- o Photographs that include pupils will be selected carefully with the permission of parents/guardians.

- o Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

- o Work can only be published with the permission of the pupil and parents/carers.

- o Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking and Personal Publishing

- The school filters do not allow access to major social networking sites.

- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils are advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school works with their broadband provider 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 e-Safety Coordinator.

Managing videoconferencing & webcam use

- Videoconferencing will be carried out using the educational broadband network to ensure quality of service and security, should the school have a need to use this medium.

- Pupils will work with a supervising teacher when making or answering a videoconference call.

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. Therefore, 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.

- The use by pupils of mobile phones or cameras in mobile phones will not be permitted.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care and supervision will be carried out in any use in school or other officially sanctioned location.

- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

Authorising Internet access

- All staff must read and sign the "Acceptable Use Agreement" 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 supervised access to suitable on-line materials.

- Parents will be asked to sign and return a consent form.

- Any person not directly employed by the school will be asked to sign an "Acceptable Use Agreement" before being allowed to access the internet from the school site.

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 can accept liability for any material accessed, or any consequences of Internet access.

- The school will 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.

- o Pupils and parents will be informed of the complaints procedure (see schools complaints policy).

- o Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- o The school will liaise with local organisations to establish a common approach to e-safety as the need arises.

Communications Policy

Introducing the e-safety policy to pupils

- o e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

- o Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- o A programme of training in e-Safety will be developed, partly based on the materials from CEOP.

- o e-Safety training will be embedded within the ICT scheme of work.

Staff and the e-Safety policy

- o All staff will be given the School e-Safety Policy and its importance explained.

- o Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

- o Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work together to resolve issues.

- o Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- o Parents and carers will be made aware of the School e-Safety policy.
- o The school will maintain a list of e-safety resources for parents/carers.
- o The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.