Cranham Church of England (VA) Primary School

E-Safety Policy

September 2014

A. Nolan

Anne Nolan (Headteacher) September 2014

Nick Ryan (Chair of Governors) September 2014

Version	Notes	Date
1	Policy re-write	September 2014

Cranham Church of England Primary School

E-Safety Policy

September 2014

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

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

- Responsible ICT use by all staff and pupils; 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 South West Grid for Learning including the effective management of web filtering.
- The school will appoint an e-Safety Coordinator.
- The e-Safety Policy and its implementation will be reviewed annually.
- The policy is approved and monitored by Governors.
- Safe Use of Internet agreements are signed by staff, pupils and parents.

TEACHING & LEARNING

Why use of the Internet 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.

Enhancing 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. Rules will be displayed and there will be targeted lessons on e-safety.
- 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, through targeted lessons, 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 recommended by SWGfL will be adopted.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive unsafe/inappropriate e-mail
- Pupils should be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain emails is not permitted.

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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing images and work

- Photographs that include pupils, carers, staff or visitors will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils', carers' or visitors' full names will not be published in digital or traditional media, particularly in association with photographs.
- Written permission from parents or carers and verbal permission from staff, governors and visitors will be obtained before photographs are published in digital or traditional media.
- Pupils' work can only be published with the permission of the pupil and parents.
- Visitors will be advised of the school e-safety policy as appropriate.

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 SWGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator. (The monitor will be switched off immediately and a member of staff will later make a note of the undesirable URL. The e-Safety co-ordinator will communicate the problem to SWGfL, so that it may be filtered out.)
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- IP videoconferencing 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 videoconference call.
- Videoconferencing 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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.
- The head teacher/deputy head teacher should be informed in instances where staff require the use of personal mobile phone to teach sessions such as assembly/PE, where **music only** maybe required.

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 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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.
- All pupil access to the Internet, in both classrooms and in the ICT Suite, will be supervised by an adult. Access will be denied during wet playtimes.
- Parents will be asked to sign and return a consent form. Pupils in Key Stage 2 will be asked to sign e-safety agreements.

Pupil mobile phones

- All staff should be aware and make both parents and children aware that if a child brings in a mobile phone into school, it must be left at the office and collected at the end of the day. **They must not be taken into class**. Teachers should not accept / offer children the choice of storing mobile devices in classrooms.
- Any mobiles confiscated from pupils who have failed to hand it into the school office, should be handed in to the school office by the member of staff and a senior member of staff should be made aware.
- All pupils and parents should be informed; children who bring mobile phones into school, do so at their own risk.
- Pupils must not take mobile phones on school trips unless prior agreement has been sought with the head teacher.

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 the Local Authority 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.

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.
- Pupils and parents will be informed of the complaints procedure.
- When suspected criminal or illegal activity has occurred (e.g. by staff or material received/found) the head will refer the matter to the Police and Local Authority.

Community use of the Internet

- The school will liaise with local organisations/ partners 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 network rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

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.

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.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating teacher web directories (Favourites) to demonstrate suitable websites that pupils will be steered towards	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Webquest UK South West Grid for Learning website
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. ∈ Ask Jeeves for kids ∈ Yahooligans ∈ CBBC Search ∈ Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History SWGfL Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum

Cranham Church of England Primary School

ICT and E-Safety Code of Conduct

Established Code March 2009

To ensure that staff are fully aware of their professional responsibilities, and for your professional and when using information systems, school laptops and the Internet, they are asked to sign this code of conduct.

- The information systems, laptop and Internet access are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my use of ICT resources and electronic information will always be compatible with my professional role.
- I understand that school information systems and property may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional rôle.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name or other personal information, those who are featured.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. Further to this I will never give out my personal address, mobile phone number etc. or that of other members of staff/school community without their express permission.
- I will not engage in any on-line activity either at home or in school that may compromise my professional responsibilities including but not limited to using social networking sites to discuss grievances relating to work or children, members of staff, comments, confidential matters or any activity that may bring the school into disrepute.
- I understand that photographs must remain on school owned cameras, encrypted and electronic devices. The permission to take school devices with photographs off site for the purposes of class related work is **ONLY** extended to **class teachers** (unless authorised by the deputy head teacher, or head teacher). In this circumstance, it is important for the class teacher to ensure photographs are kept on and worked off school owned devices and never stored on own personal devices. Furthermore, photographs and equipment must be brought back into school on the following day and must not be left at home.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that by signing this Code of Conduct I am responsible for my actions both in and out of school: I understand that this applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Code of Conduct, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority, dismissal and in the event of illegal activities the involvement of the police.

- If I have any concerns about the application of this code I will consult the e safety coordinator (the designated child safeguarding lead): Mrs. Anne Nolan.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.