St Robert Southwell Primary School
E-Safety Policy

Governors' Committee Responsible		Resources	
Policy Editor	ICT Leader/School Business Manager	Review Period	Bi-Annual
Status	Recommended	Date Approved	Summer 2016
Version History	V01	Next Review Date	Summer 2018

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.

- The school will appoint an e-Safety Coordinator. In many cases this will be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed bi-annually.
- The e-Safety Policy was revised by: L Willsher

Teaching and Learning

Why 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 students with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access is currently provided by West Sussex County Council and includes filtering appropriate to the age of the 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.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to 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 how to report unpleasant Internet content.

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.

Email

- **Pupils and staff may only used approved email accounts on the school system. At present all email facilities used by pupils in school will be for education purposes only.**
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in any e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication will only be related to school and must only take place via a school email address and will be monitored.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The content details on the website should be the school address, email and telephone number. Pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully. The school will seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the website as appropriate, including blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords and internet safety presentations. Currently these sites are blocked by the schools' filtering system.
- Newsgroups will be blocked unless a special 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 networking spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing Filtering

- The school will work in partnership with West Sussex 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.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Videoconferencing

- Videoconferencing will 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 by ICT Leader before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with parents/pupils is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All personal data will be encrypted if being stored on portable devices.
- Personal data will only be used (or saved) on encrypted memory sticks and school computers.

- With the integration of remote access, data will not need to be removed from the premises as it can be saved on school network and accessed from home. This enables our data to remain secure.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any 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 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 of school ICT resources' form before being allowed access to 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 Internet content, it is not possible to guarantee unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The ICT leader will audit ICT use to establish if the e-Safety policy is adequate 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 head teacher.
- Complaints of a child protection nature must be dealt with school child protection procedures.
- Pupils and parents will be informed of the 'managing parental concerns' procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-Safety policy.

Communications Policy

Introducing the e-Safety policy to pupils

- Appropriate elements of the e-Safety policy will be shared with pupils.
- E-Safety rules will be posted on all networked rooms including classrooms and hall.
- An e-Safety assembly will be held annually, if not more often, to encourage safe use of the Internet.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-Safety issues and how best to deal with them will be provided for pupils yearly.

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.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on e-Safety.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- The school will provide parents with details on e-Safety events they may wish to attend.

Top Tips!!

- Use internet filtering software and child-friendly search engines
- Keep the computer in a communal area of the house, where it's easier to monitor what your children are viewing.
- Tell children not to give out their personal details
- Children love to chat, but make sure they only use moderated chat rooms and encourage them to introduce you to their online friends.
- Encourage your children to tell you if they feel uncomfortable, upset or threatened by anything they see online.
- Involve your children in writing your own family code of acceptable internet use.
- Remember that what's acceptable for a teenager isn't necessarily OK for a primary school-aged child, so get their input.
- The web's a great resource for homework, but remember to use more than one site in research.
- Surf together. Go online with your children and become part of their online life. The key to safe surfing is communication.