



The Federation of Swale Catholic Primary Schools

Chair of Governors: Cllr. Duncan Dewar-Whalley

Clerk to the Governors: Mrs Julie Hardy



✉ governors@st-peters-sittingbourne.kent.sch.uk

e-Safety Policy

This e-Safety Policy is part of St. Edward's and St. Peter's Catholic Primary school's improvement plans and relates to other policies including those for ICT, Anti-Bullying, Behaviour Management, Curriculum and for Child Protection. The Executive Headteacher, who is one of the Designated Child Protection Co-ordinator, is also the e-Safety Co-ordinator, working closely with the ICT Subject Leaders to develop an effective approach to managing e-Safety issues.

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

Our e-Safety Policy and its implementation will be reviewed annually.

It was approved by Governors on:

Teaching and Learning:

The purpose of Internet use in schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

Benefits of using the Internet include:

- access to world-wide educational resources including museums and galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support, including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with KCC and DCSF;
- access to learning wherever and whenever convenient.

Use of the Internet to enhance learning:

St. Edward's and St. Peter's Catholic schools Internet access will be designed expressly for pupil use and will include 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. 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.

Evaluation of Internet content by pupils:

St. Edward's and St. Peter's Catholic schools 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.

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 Kent EIS.

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.

Published content and the school website:

- ✓ The contact details on the website should be the school address, e-mail and telephone. Staff or pupils' personal information will not be published.
- ✓ The Executive Headteacher 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 and will not enable individual pupils to be clearly identified.
- ✓ Pupils' full names will not be used anywhere on the website or Blog, particularly in association with photographs.
- ✓ Written permission from parents or carers will be obtained before photographs of pupils are published on either schools website.
- ✓ Pupil's work can only be published with the permission of the pupils and parents.

Social networking and personal publishing:

- St. Edward's and St. Peter's Catholic schools 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:

- St. Edward's and St. Peter's Catholic schools will work with the Local Authority, DCSF and the Internet Service Provider 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 Co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing:

St. Edward's and St. Peter's Catholic schools have not yet introduced videoconferencing but as the pace of change with technology is so rapid and the cost of web cameras has fallen, use of videoconferencing has been included as it could be introduced in the foreseeable future, before the annual review of this policy.

- Internet Protocol (IP) videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet, as IP technology is used in a secure and managed environment.
- Pupils should ask permission from the supervising teacher/teaching assistant 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 carried out before use in school is allowed.
- Mobile phones are not allowed for pupils in St. Edward's (pupils walking home surrender to office for safekeeping) or St. Peter's Catholic schools.
- Pupils may have mobile phones at home and they should be made aware that sending abusive or inappropriate text messages is unacceptable and could be classed as bullying.
- Staff will be issued with a school phone where contact with pupils is 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 User Agreement' before using any school ICT resource.
- ✓ St. Edward's and St. Peter's Catholic schools will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date e.g. a member of staff may leave or a pupil's access can be withdrawn.
- ✓ At Key Stage 1, access to the Internet will be adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- ✓ Parents will be asked to sign and return a consent form.

Assessing risks:

- ✓ St. Edward's and St. Peter's Catholic schools 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 KCC 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 complaints about staff misuse must be referred to the Executive 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.
- ✓ Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet:

St. Edward's and St. Peter's Catholic schools 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 networked rooms and classes with Internet access, and discussed with pupils at the start of the year.
- ✓ Pupils will be informed that network and Internet use will be monitored.

Staff and e-Safety Policy:

- ✓ All staff will be given the 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 schools e-Safety Policy in newsletters, the school brochures and on the school websites.

Appendix 1: Internet use – Possible teaching and learning activities

Activities	Key e-Safety Issues	Relevant Websites
Creating web directories to provide easy access to suitable websites	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials	Web directories e.g. Ikeep bookmarks Webquest UK Webplay Kent Grid for Learning (Tunbridge Well Network)
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. <ul style="list-style-type: none"> ▪ Ask Jeeves for kids ▪ Yahoo!igans ▪ CBBC Search ▪ Kidsclick Webplay
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 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 & Galleries CC4G Espresso Webplay
Publishing pupils' work on school and other websites.	Pupil and parent consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on film CC4G Espresso Webplay
Publishing images, including photographs of pupils.	Parental consent for publication of photograph 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 Learning grids Museum sites etc Digital Storytelling BBC – Primary Art Webplay
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 CC4G Webplay
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 National History Museum Imperial War Museum Webplay

Our School e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:

Form:

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:

Date:

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Please print name:

Please complete, sign and return to the school secretary

Think then Click

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



B. Stoneham & J. Barrett

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Appendix 3: Staff Information Systems Code of Conduct

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems 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 information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Executive Headteacher.
- 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 role.
- 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.

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.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: Capitals: Date:

Accepted