

St Michael's Church of England Primary School



E-Safety Policy

OUR MISSION STATEMENT

At St Michael's Primary School we seek to nurture the whole child and instil a love of learning by inspiring young minds within a happy, caring community based on the Christian values of love; joy; kindness; peace; self-control and faithfulness.

Introduction

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.

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

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection.

* The school will appoint an e-Safety Coordinator. This responsibility will be shared by the Designated Child Protection Coordinator and the ICT Coordinator.

* 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.

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

* The e-Safety Policy was revised by the SLT

Teaching and learning

Why is Internet use 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.

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

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art 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 DFE;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Developing effective practice in Internet use for teaching and learning is essential. Teachers can help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

- The school Internet access is designed expressly for pupil use and includes 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.
- Staff will 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.

How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. Information received via the Internet, e-mail or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. A whole curriculum approach may be

required. In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed.

It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher. More often, pupils will be judging reasonable material but will need to select relevant sections. Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas. Some filtering software can provide temporary access to specific sites, which a teacher considers necessary for a particular purpose. Clearly pupils need to understand that unselective copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- 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.

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 KCC (EIS).

E-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created. The implications of e-mail use for the school and pupils need to be thought through and appropriate safety measures put in place. Un-regulated e-mail can provide routes to pupils that bypass the traditional school boundaries.

- 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.
- The forwarding of chain letters is not permitted

Published content and the school web site

School websites can inspire pupils to publish work of a high standard. Websites can celebrate pupils' work, promote the school and publish resources for projects. Sensitive information about staff and pupils should not be accessed through 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 headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully
- 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.
- Pupils in photographs should be appropriately clothed.

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, with the exception of those recommended by school, is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DFE 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 Coordinator

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

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.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form to permit Internet access.

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 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 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.

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 posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

Staff and the e-Safety policy

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff and governors should include a discussion of the school's 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 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 Kent Grid for Learning (TW 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
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 Kent Grid for Learning 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

Appendix 2

e-Safety Contacts and References

CFE e-Safety Officer, KCC Children Families & Education

e-mail: esafety@kent.gov.uk Tel: 01622 696590

Kent Community Network Helpdesk Children's Safeguards Service Help with filtering and network security. www.clusterweb.org.uk?safeguards www.eiskent.co.uk (broadband link)

Tel: 01622 206040

BBC Chat Guide

<http://www.bbc.co.uk/chatguide/>

Becta

<http://www.becta.org.uk/schools/esafety> **Childline**

<http://www.childline.org.uk/> **Child Exploitation & Online Protection Centre**

<http://www.ceop.gov.uk>

e-Safety in Schools

<http://www.kenttrustweb.org.uk?esafety>

Grid Club and the Cyber Cafe

<http://www.gridclub.com>

Internet Watch Foundation

<http://www.iwf.org.uk/>

Internet Safety Zone

<http://www.internetsafetyzone.com/> **Kent Primary Advisory e-Safety Pages**

<http://www.kented.org.uk/ngfl/ict/safety.htm>

Kidsmart

<http://www.kidsmart.org.uk/> **NCH – The Children's Charity**

<http://www.nch.org.uk/information/index.php?i=209> **NSPCC**

<http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm> **Schools e-Safety Blog**

<http://clusterweb.org.uk?esafetyblog>

Schools ICT Security Policy

<http://www.eiskent.co.uk> (broadband link) **Stop Text Bully**

www.stoptextbully.com

Think U Know website

<http://www.thinkuknow.co.uk/>

Virtual Global Taskforce – Report Abuse

<http://www.virtualglobaltaskforce.com/>

Children's Officer for Training & Development, Child Protection Mike O'Connell

e-mail: mike.oconnell@kent.gov.uk Tel: 01622 696677

Appendix 3



Key Stage 1



Key Stage 2

Appendix 4

<p>Our School e-Safety Rules</p> <p><i>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.</i></p>	
<p>Pupil:</p>	<p>Year:</p>
<p>Pupil's Agreement</p> <ul style="list-style-type: none"> ● 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. 	
<p>Signed:</p>	<p>Date:</p>
<p>Parent's Consent for Web Publication of Work and Photographs</p> <p>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.</p>	
<p>Parent's Consent for Internet Access</p> <p>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.</p> <p>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.</p>	
<p>Signed:</p>	<p>Date:</p>
<p>Please print name:</p>	
<p>Please complete, sign and return to the school secretary</p>	

--

Appendix 5

E-Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an e-Safety Policy that complies with CFE guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both students and staff?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for students?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access (e.g. the Kent Community Network).	Y/N
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
