St. Anne's & St. Joseph's R.C. Primary School

e-SAFETY POLICY

Jesus is " a light that shines in the dark' a light that darkness could not overpower."

John 1:5

This 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 has a role of e-Safety Coordinator which is jointly undertaken by Mrs Holden (Child Protection Senior Management Team Member) and Mrs Hunter (ICT Coordinator)

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

This e-Safety policy was revised by Mrs A Hunter

It was approved by Governors during the Autumn term 2008.

The next review date is Autumn 2009.

TEACHING AND LEARNING

Why the 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 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.

Internet use will enhance learning

The school Internet access has been designed expressly for pupil use and includes filtering appropriate to the age of the pupils as supplied by the Lancashire Schools ICT Centre.

Pupils will be taught what Internet use is acceptable and what is not and will be 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 to a wider audience.

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 will be taught the importance of cross-checking 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 Lancashire ICT Schools Centre.

E-mail

Pupils are currently taught how to use e-mail using a closed system (2Simple E-mail) however the introduction of Moodle into school will necessitate pupils being given e-mail accounts of their own. A decision will then be taken at Senior Management level regarding which pupils if any, will have access to e-mail accounts via the world wide

web. If external e-mail systems are approved the following will form the basis of its use.

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

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

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider how e-mail from pupils to external bodies is presented and controlled.

The forwarding of chain letters in not permitted.

Published content and the school web site

Staff or pupil personal contact information will not be published. Contact details given online should only be the school office.

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 so that individual pupils cannot be identified or their image misused. Consideration will be given to using group photographs rather than full face photos of individual children.

Pupil's full names will not be used anywhere on the school web site or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs are used in any media. See school policy for photographing of pupils.

Work can only be published with the permission of the pupil and parent/carers.

Pupil image file names will not refer to the pupil by name.

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use.

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, their friends or their location.

Pupils and parents will be advised that the use of social network 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 with Lancashire Schools ICT Centre to ensure systems to protect pupils are continually 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 and webcam use

Videoconferencing should use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconferencing call.

Videoconferencing and webcam use will be appropriately supervised for the pupil's 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.

The senior management 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.

Mobile phones will not be used during lessons or formal school time. All mobile phones brought into school will be stored in the Secretary's office during school hours and returned to pupils at the end of the school day. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by pupils of cameras in mobile phones is not permitted at any time on school premises.

Games machines including Sony Playstation, Microsoft Xbox and others have Internet access, which may not include filtering. As such they should not be brought into school at any time.

Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils for school use.

The appropriate use of Learning Platforms (Moodle) 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.

POLICY DECISIONS

Authorising Internet access

All staff must read and sign the "Staff Code of Conduct for ICT" before using any school ICT resource. (See attached appendix)

The school will maintain a current record of 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 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. Neither the school nor LCC can accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use as and when necessary 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 will be dealt with in accordance with school child protection procedures.

COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

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

Pupils will be informed that network and Internet use will be monitored and inappropriate use will be followed up.

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

e-Safety training will be embedded within the ICT scheme of work and or the Personal Social and Health Education (PHSE) curriculum.

Staff and the e-safety policy

All staff will be given the School e-safety policy and its importance explained.

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

Staff will always use a child friendly safe search engine when accessing the web with children such as Ask Jeeves for Kids, Yahooligans, CBBC Search or Kidsclick.

Enlisting parents' and carers' 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.

The school will maintain a list of e-safety resources for parents and carers.

The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Appendix 1: Internet use – Possible teaching and learning activities

Activities	Key e-safety issues	Relevant website
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 eg Ikeep bookmarks Webquest UK The school VLE (Moodle)
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. 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.	Ask Jeeves for Kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information.	RM EasyMail SuperClubs Plus Schools Net Global Kids Safe Mail
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. Pupil's work should only be published on "moderated sites" .	Making the News SuperClubs Plus Learninggrids Museum sites etc Digital Storytelling BBC - Primary Art Cluster Microsites
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual children to be identifies. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites etc Digital Storytelling BBC - Primary Art Cluster Microsites
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 Plus FlashMeeting
Audio and video conferencing to gather information and share pupils' work	Pupils should be supervised. School should only use applications that are managed by Lancashire Schools ICT Centre	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Key Stage 1

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

Key Stage 2

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 are 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

Staff Code of Conduct for ICT

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

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems my not be used for private purposes without specific permission from the Headteacher.

- I understand that my use of school information systems, Internet and e-mail may be monitored and recorded to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.

- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken of 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 e-Safety Coordinator, the Designated Child Protection Coordinator or the Headteacher.

- I will ensure that electronic communications with pupils, including e-mail, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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 accept the Staff Code of Conduct for ICT.

Signed: …… Print:…… Date: ……

For school: ……. Print: …… Date: ……

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 this form to show that the e-Safety rules have be understood and agreed.

Pupil: …… Class: ……

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 Internet Access

I have read and understood the school e-Safety rules and give my permission for my child 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 school as soon as possible.