St Mary's Catholic Junior School

E-Safety Policy

This policy is to be read in conjunction with the following policies: Safeguarding & Child Protection, Positive Behaviour Policy, Home School Agreement, Data Protection.

Author: L Durrant
Date Prepared: May 2011
Date Approved: November 2011
Date of Review: November 2013

Contents

UNIT 01 **Introduction**

The Primary eSafety Policy

This core eSafety policy provides a basic template for the schools policy and has been approved by the Sutton Local Safeguarding Children's Board.

Effective Practice in eSafety

eSafety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented eSafety Policy
- Secure, filtered communications provided by the SWAN Network
- A school network that complies with the National Education Network standards and specifications.

UNIT 02 *ESafety Audit – Primary & Special schools*

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for eSafety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, eSafety Coordinator, Network Manager and Head Teacher.

Does the school have an eSafety policy that complies with Sutton guidance? Y/N

Date of latest review (at least annual):

The school eSafety policy was agreed by governors on:

The policy is available for staff at:

The policy is available for parents and carers at:

The responsible member of the Senior Leadership Team is:

The responsible member of the Governing Body is:

The Designated Child Protection Coordinator is:

The eSafety Coordinator is:

Has eSafety training been provided for both pupils and staff? Y/N

Is there a clear procedure for a response to an incident of concern? Y/N

Have eSafety materials from CEOP and Becta been obtained? Y/N

Do all staff sign a Code of Conduct for ICT on appointment? Y/N

Are all pupils aware of the school's eSafety Rules? Y/N

Are eSafety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? Y/N

Do parents/carers sign and return an agreement that their child will comply with the School eSafety Rules? Y/N

Are all staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? Y/N

Is personal data collected, stored and used according to the principles of the Data Protection Act? Y/N

Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. SWAN)? Y/N

Has the school web filtering policy been designed to reflect educational objectives and approved by SLT? Y/N

UNIT 03 The school eSafety Policy

3.1 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 eSafety Coordinator.** This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
- Our eSafety Policy has been written by the school, building on the Sutton eSafety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by: **Lucy Durrant**
- It was approved by the Governors on:
- The next review date is (at least annually): **June 2012**

3.2 Teaching and learning

3.2.1 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.

3.2.3 Internet use will enhance 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.

- 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 (e.g. MLE).

3.2.4 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 e.g. using the CEOP Report Abuse icon or Hector Protector.**

3.3 Managing Internet Access

3.3.1 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.

3.3.2 Email

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how email from pupils to external bodies is presented and controlled.

3.3.3 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- **The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.**

3.3.4 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. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, 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.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

3.3.5 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.
- **Ideally pupils would use only moderated social networking sites, e.g. SuperClubs Plus**

- 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.

3.3.6 Managing filtering

- The school will work with the LA and SWAN 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.

3.3.7 Managing videoconferencing & 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 videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

3.3.8 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 leadership 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. 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 will be kept under review.**
- **Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.**
- 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.
- The appropriate use of Managed Learning Environments will be discussed as the technology becomes available within the school.

3.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3.4 Policy Decisions

3.4.1 Authorising Internet access

- All staff must read and sign the Staff ICT Acceptable Use Policy before using any school 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 the ICT Acceptable Use Policy before being allowed to access the internet from the school site.**

3.4.2 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 LA can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate and effective.

3.4.3 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 (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

3.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to eSafety.

3.5 Communicating eSafety

3.5.1 Introducing the e-safety policy to pupils

- eSafety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.
- eSafety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

3.5.2 Staff and the eSafety policy

- All staff will be given the School eSafety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

3.5.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- **The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.**

UNIT 03 *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 Learning Zone The school / cluster VLE
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.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via email or blogs.	Pupils should only use approved email accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	SWAN Email service The London MLE
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. Pupils'work should only be published on moderated websites by the school administrator.	Making the News SuperClubs Plus Headline History Cluster Microsites National Education Network Gallery
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. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
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. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)