English Martyrs'
RC Primary School

E-Safety Policy

MISSION STATEMENT

Our English Martyrs' School community
aims to follow the example of Christ
in welcoming, recognising, fostering and developing each individual
as a unique and special gift of GOD with value and dignity.

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

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

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

E-Safety Audit – Primary Schools

This quick self-audit will help the senior leaders team (SLT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	
Date of latest update: Sept 2020	
The Policy was agreed by governors on: Sept 2020	
The Policy is available for staff at: On network server	
And for parents at: School's website	
The designated Child Protection Teacher/Officer is: Ms Akpjotor	
The e-Safety Coordinator is: Mr Humphreys	
Has e-safety training been provided for pupils, parents and staff?	**Yes**
Is the Think U Know training being considered?	**Yes**
Do all staff sign an ICT Code of Conduct on appointment?	**Yes**

Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	**Yes**
Have school e-Safety Rules been set for pupils?	**Yes**
Are these Rules displayed in all rooms with computers?	**Yes**
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	**Yes**
Has the school filtering policy been approved by SLT?	**Yes**
Is personal data collected, stored and used according to the principles of the GDPR Act?	**Yes**

Contents

School e-Safety Policy

The school will appoint an e-Safety coordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap.

Our e-Safety Policy has been written by the school, building on the Southwark Children and Young Peoples' Directorate & Commission for schools and Colleges of Southwark Diocese and Government guidance. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed November 2021.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet 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;
- 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 the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be 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.

- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign a consent form for pupil access on admission.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- 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.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations 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.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups 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 should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- 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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Cameras in mobile phones are not used by staff or pupils.
- Only school cameras and iPad camera are used by both staff and children for educational purposes.

Published Content and the School Web Site

- 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 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 and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission will be required from parents of pupils who do not want their child/ren's photographs to be used on the school Web site or published in newsletter or yearbook
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

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 that unsuitable material will never appear on a school computer. Neither the school, Commission for schools and Colleges of Southwark Diocese nor Southwark Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms near computers.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will have access of the School e-Safety Policy on the network server 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.

Parents

- Parents' attention will be drawn to the School e-Safety Policy at Meet the Teachers meeting, in newsletters, the school brochure and on the school's website.

Policy for the Use of Facebook and other Social Networking Sites

Aims

The aim of this policy is to set clear guidelines for the use of Facebook by staff, pupils and parents.

Introduction

Facebook is a popular Social Networking site which has been running since 2004:
www.facebook.com

Facebook is only for users aged 13 or over, however it is very easy for young people (or indeed adults) to enter an incorrect date of birth or false information to open an account.

It is essential that, if children under the age of 13 are using Facebook, they need to be aware of how to protect their information, how to report abuse or inappropriate content and that their parents/carers must be aware that they are online. School ensures that all children in KS2 receive e-safety talks. Parents are also invited to attend these talks.

With such a publicly accessible system it is open to abuse by all users. Parents are guilty of publishing critical comments about staff, children and other parents. Children can leave themselves open to abuse from other children and adults as well as being abusive about staff and other children. Staff can also be guilty of making comments about other staff, parents and children. This can sometimes be done in the belief that the correct privacy settings are in place.

Social Media platforms

Staff

Staff are within their rights to use Facebook and other social media platforms and we are not, nor would not want to be, in a position to prevent staff from using the site. However, we do ask that staff adhere to the following rules:

- Under no circumstances should pupils or ex-pupils under the age of 13 be accepted as a friend. Failure to follow this will result in disciplinary action being taken. If a child requests a member of staff as a friend then their parents must be informed and they should be reported to Facebook for being under age.

- Staff are asked to use extreme caution if a parent makes contact through Facebook. In the event of communicating with a parent or adult associated with a child who attends the school, no comments should be made about children, staff or parents. If a member of staff is found in breach of this rule then disciplinary action may follow.

- Any statements or status remarks should again not contain any comments about the school, staff, parents or children. If a member of staff is found in breach of this rule then disciplinary action may follow.

Children

Under no circumstances should children access Facebook in school or other social media platforms. The school network system prohibits children from accessing the site but the bypassing of the system or accessing through a mobile phone will result in exclusion.

If any reports are received of children making comments about staff or other children, hard copies will be obtained and the child will be reported immediately to Facebook to have their account cancelled. The parents/carers of the child will also be notified and this could result in exclusion. If the comment is about a member of staff a referral will be made to the County's legal services.

Parents

If hard copies of inappropriate comments about members of staff or other children within school are received then the matter will be referred to the County's legal services and subsequent action will follow.

Parents must not, under any circumstances, access their Facebook accounts whilst assisting on school visits. If there is evidence to prove that this has happened then the parent will no longer be used as a helper on subsequent visits.

Referral Process – Appendix A

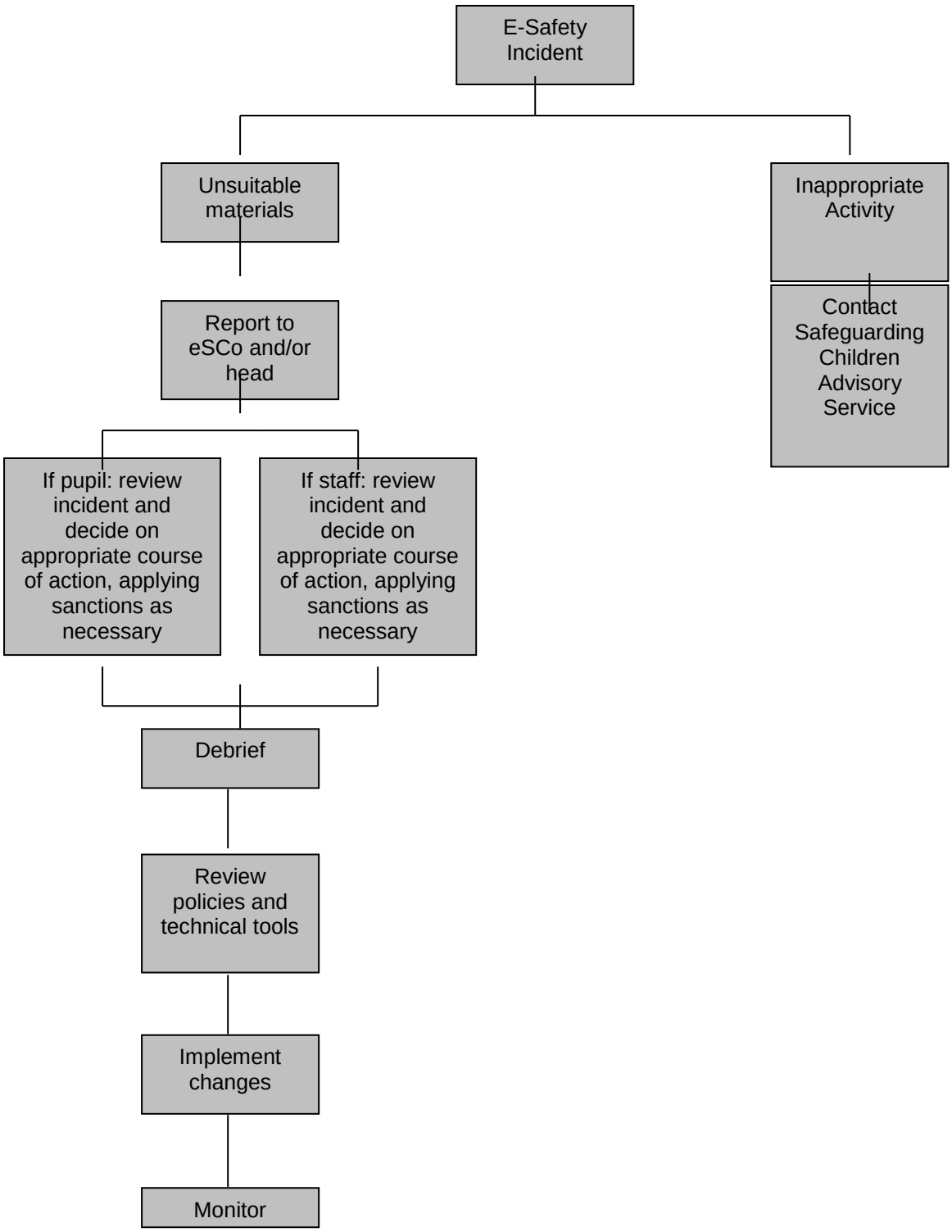
E-Safety Rules– Appendix B.1, 2, 3

Letter to parents – Appendix C

Staff Acceptable Use Policy – Appendix D

Appendix A

Flowchart for responding to e-safety incidents in school



Appendix B .1 **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.

Appendix B.2

e-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Appendix B.3

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. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

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:	
Child's Class	

Please complete, sign and return to the school

Appendix D

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 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 pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not make comments about the school, staff or pupils or post pictures of pupils on any social network site.

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.

Name: …… Signed: …… Date: ……

Accepted for: English Martyrs School - By: ……