St. Mary's
Catholic Federation

St Mary's Catholic Federation, Carshalton

Learning, playing and growing together in the love of Jesus

E-Safety Policy
Non – Statutory
(Bi – Annually)

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

Author: E-Safety Leads
Committee - SLT
Date Prepared: February 2023 - No changes made
Date Approved: July 2023
Date of Review: November 2024
Approved by the Full Governing Body Date: July 2023

Chair of Governors Signature:

Safeguarding Statement
This school takes notice of and adheres to all the national and local policies and guidance in regard to Safeguarding Children and Young People.

Lead Safeguarding Person Junior School: Mrs M Kenny

Lead Safeguarding Person Nursery & Infant School: Mrs M Quinn

Safeguarding Deputies: (Infants) - Mrs S Hulme & Mrs E Heath **(Juniors) -** Mrs S Hulme, Mrs F Black & Mr S Pratsis

Governor designated safeguarding officer: Mr. T Richmond

"St Mary's is committed to being a Rights Respecting School to inspire and support the children, parents and school governors in school and the wider community."

Contents

1. Introduction

The Primary E-Safety Policy

This core E-Safety policy provides a basic template for the school policy and has been approved by the Sutton Local Safeguarding Children's Board.

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible Computing use by staff and pupils.
- A comprehensive, agreed and implemented E-Safety Policy.
- Secure, filtered communications provided by the Cygnet IT, LGFL Network and Google.
- A school network that complies with the National Education Network standards and specifications.

2. E-Safety Audit – Primary schools

This self-audit should be completed by the subject leader in collaboration with a member of the Senior Leadership Team (SLT) responsible for E-Safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, E-Safety Coordinator, Network Manager from Cygnet and Head Teacher.

Does the school have an E-Safety policy that complies with Sutton guidance? **Y/N**

Date of latest review (at least annual):

The school E-Safety 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 E-Safety Coordinator is:

Has E-Safety 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 E-Safety materials from CEOP and ThinkUknow been obtained? **Y/N**

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

Are all pupils aware of the school's E-Safety Rules? **Y/N**

Are E-Safety 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 E-Safety 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 Cygnet requirements (e.g. Cygnet and LGFL)? **Y/N**

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

3. The school E-Safety Policy

3.1 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 Computing, Bullying, Safeguarding & Child Protection, Positive Behaviour Policy, Home School Agreement, Data Protection and Equal Opportunities.

- The school appointed E-Safety Coordinator is Miss Santos & Mr Awadalla.
- Lead Safeguarding Person Junior School: Mrs M Kenny

  Lead Safeguarding Person Nursery & Infant School: Mrs M Quinn

  Designated Child Protection Co-ordinator: Mrs M Kenny.

  E-Safety Safeguarding Person Junior School: Mrs M Kenny

  It is not a technical role.
- Our E-Safety Policy has been written by both schools, building on the Sutton E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The E-Safety Policy was revised by: **Miss Santos & Mr Awadalla**
- It was approved by the Governors on: **July 2023**
- The next review date is (at least annually): **November 2024**

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. Google Workspace for Education).

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 through Computing and PSHE and E-Safety sessions (Juniors - twice a term) and E-Safety Week.

➢ In Years 3-6 they will be taught through a scheme of work **Be Internet Legends and Interland https://beinternetawesome.withgoogle.com/en_us/interland and Cyberpass - LGFL https://www.lgfl.net/learning-resources/summary-page/cyberpass**

At the Juniors this is taught twice a term.

➢ Years 1 to 6 - will be taking part in the E-Safety week by a talk with Steve Welding (if possible).

3.3 Managing Internet Access

3.3.1 Information system security

- School Computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Cygnet who provide the first level of security and Google providing the second.

3.3.2 Email

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an 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.
- Using G-Mail pupils can only email within the domain stmarysfed.uk
- The school should consider how email from pupils to external bodies is presented and controlled.

3.3.3 Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Head Teacher will take overall editorial responsibility and ensure that the 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 Website or other on-line space, particularly in association with photographs.

- Written permission from parents/carers will be obtained before photographs of pupils are published on the school Website, for use in Google Workspace for Education and at any public events.
- 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.
- 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 and on Google Workspace for Education.

3.3.6 Managing filtering

- The school will work with the Cygnet 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 Cygnet, the E-Safety Coordinator and SLT.
- 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 video conferencing & webcam use

- Video conferencing 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 video conference call and only if a teacher is present.

- Video conferencing and webcam use will be appropriately supervised for the pupils' age.
- Use of Google Meet for Online Registration during school closure and with cameras off. Twice a week. Guidance given to staff and parents of how to behave online.

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.
- Only pupils in Year 6 have the permission to bring mobile phones to school for Emergency communication before and after school. During the school day the mobiles are held in the office and are signed in and out by each pupil.
- Games machines including the Sony Playstation, Microsoft Xbox, Nintendo Switch, Nintendo 2DS and 3DS and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- No staff mobile phones are used to capture photographs of pupils.
- The appropriate use of Google Workspace for Education will be discussed as the technology becomes available within the school.
- St. Mary complies with the General Data Protection Regulation (GDPR) and regualies keeps updated with any new legislation.
- Smart Watches - Apple watch, android watch etc will be reviewed by SLT if it is appropriate or necessary for school.

3.3.9 Protecting personal data

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

- St. Mary complies with the General Data Protection Regulation (GDPR) and regualies keeps updated with any new legislation.

3.10 Recording of performances

- All recording of any musical performances must not be recorded on any device unless requested permission by the school. Before a performance commences a child asks the audience that all electronic devices be switched off to keep the children safe. Prior to the performance being performed and recorded by the school a letter will go out to inform parents if they wish for the performance to be recorded. If any parent/s does not wish the performance to be recorded by the school then no recording will be made which is in line with our Safeguarding Policy.

3.4 Policy Decisions

3.4.1 Authorising Internet access

- All staff must comply with the regulations of the school when using computing systems/devices.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- Any person not directly employed by the school will be asked to comply with the regulations of the school when using computing systems/devices.

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

3.4.3 Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by SLT staff and Designated Safeguarding officers.
- 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 school's 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 Cygnet to establish a common approach to E-Safety.

3.5 Communicating E-Safety

3.5.1 Introducing the E-Safety policy to pupils

- E-Safety 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 Be internet legends and CEOP.
- E-Safety training will be embedded within the Computing scheme of work or the PSHE curriculum through lessons twice a term at the Juniors and Safer Internet Day at both schools through the scheme of work by LGFL Cyberpass **https://www.lgfl.net/learning-resources/summary-page/cyberpass** and Be Internet Legends and Interland **https://beinternetawesome.withgoogle.com/en_us/interland** which will be taught in Years 3-6.

3.5.2 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 network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor Computing 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 E-Safety Policy in newsletters, the school brochure and on the school Website.
- E-Safety meetings will be held twice a year, once at the Infants and once at the Juniors with the Education E Safety Adviser presenting information about current trends in E-Safety. Once a year workshops will be given by the Education E Safety Adviser either to a whole year group or to individual classes.
- 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.
- Termly newsletters include a E-safety section updating parents with any new websites. E.g:

  https://www.nspcc.org.uk/
  http://www.thinkyouknow.co.uk/
  http://www.internetmatters.org/
  http://www.kidsmart.org.uk/
  http://www.childnet.com/
  https://www.commonsensemedia.org/

4. 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 The school / Google Classroom
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought.	Web quests e.g. CBBC Search Kidsclick

	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.	
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.	LGFL Email G-Suite
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 Video conferencing

Self Audit E-Safety Autumn 2022

Does the school have an E-Safety policy that complies with Sutton guidance?	**Y/N**
Date of latest review (at least annual): December 2022	
The school E-Safety policy was agreed by governors on: Tim Richmond	
The policy is available for staff at: Federated Curriculum on Google Drive	
The policy is available for parents and carers at: School website	
The responsible member of the Senior Leadership Team is: Maeve Kenny	
The responsible member of the Governing Body is: Tim Richmond	
The Designated Child Protection Coordinator is: Maeve Kenny and Marcelle Quinn	
The E-Safety Coordinators is: Miss Santos & Mr Awadalla	
Has E-Safety 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 E-Safety materials from CEOP and ThinkUknow been obtained?	**Y/N**
Do all staff sign a Code of Conduct for Computing on appointment?	**Y/N**
Are all pupils aware of the school's E-Safety Rules?	**Y/N**
Are E-Safety 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 E-Safety 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 and GDPR?	**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with Cygnet requirements (e.g. Cygnet and LGFL)?	**Y/N**
Has the school web filtering policy been designed to reflect educational objectives and approved by SLT?	**Y/N**