St. Mary's Catholic Primary School Chiswick

"Living and learning, inspired by our faith"

E-SAFETY POLICY

September 2020

_____ _____

Headteacher / Chair of Governors **Date**

Next Review Date: August 2022

1. Introduction

1.1. This policy is written with the understanding that the benefit provided to children by modern technologies is indispensable and that these technologies are an invaluable tool in teaching and learning both in and out of school.

1.2. Computing supports the professional work of staff and enhances the school's management information and business administration systems.

1.3. It is an entitlement for all students as it helps them to develop a responsible and mature approach to accessing information. Without technology, truly effective teaching and learning would not be possible here at St Mary's.

1.4. It is also understood that with this great potential comes a small element of risk, which can be avoided if properly addressed by adults in school, children and parents.

2. What is E-safety?

2.1. E-safety broadly speaking means the safe use of any digital media. E-safety encompasses the internet, personal computers, digital cameras, mobile phones (especially those with camera and internet capability), digital music players and recorders, and portable digital memory storage (memory cards etc.).

2.2. E-safety does not mean dramatically restricting children's use of digital technology, instead we hope that through certain safeguards and increased awareness children are able to make full and safe use of this technology.

3. Safeguards within school

3.1. Internet

3.2. Our school is equipped with sophisticated filtering and firewall systems to ensure that as far as possible children are protected from unsafe web browsing. The school will work with the LEA and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.

3.3. Children are not permitted to use the internet unless supervised by an adult.

3.4. Children will be shown appropriate sites and responsible strategies for using the internet in school.

3.5. If staff or students discover unsuitable sites, the URL (address) and content will be reported to the network manager / ICT coordinator, London Grid for Learning (LGfL) or LEA as appropriate;

3.6. Any material that the school suspects is illegal will be referred to the appropriate authorities.

4. Use of E-mail

4.1. From Key Stage 2, pupils are expected to use E-mail as part of the National Curriculum.

4.2. Pupils may send E-mail only as part of planned lessons.

4.3. Pupils will only be given 'safe' email accounts through the London Grid for Learning or other approved Supplier; younger children will only use a managed virtual email programme, such as 2Email.

5. The School Website

5.1. The Headteacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained;

5.2. The web site will comply with the school's guidelines for publications;

5.3. Pupils will be taught to publish for a wide range of audiences which might include governors, parents or young children;

5.4. All material must be the author's own work, credit the sources used and state clearly the author's identity or status;
5.5. The point of contact on the web site will be the school address and telephone number. Home information or individual E-mail identities will not be published;
5.6. The school website will not reveal any specifics about children [and if a photo is featured, the names will not be given, and vice versa].

6. The School Network

6.1. The staff areas of the networked computers [wherein confidential or personal data are stored] are inaccessible to children. Adult workstations will be locked when not in use.
6.2. Virus protection will be installed and updated regularly;
6.3. As a school we will ensure that all staff sign and abide by the Acceptable Use Policy. Any breaches of this agreement will be dealt with accordingly [see How will incidents be handled? section below.]
6.4. Specific information or photos of children will be inaccessible to non-staff.
6.5. The network manager will perform regular checks on staff and pupil computer use, and report any irregularities accordingly.

7. Teaching of E-safety

7.1. We acknowledge that with even the most vigilant E-safety practices in place, the ultimate safeguard lies in cultivating a wise and well-informed cohort and staff.
7.2. Before any internet use, teachers will prepare and drill children on E-safety practises.
7.3. Regular checks on student awareness will be carried out.
7.4. Staff will be given a checklist and regular reminders of E-safety requirements.
7.5. An annual E-safety week will involve assemblies lead by senior staff, and individual lessons that are followed up everyday throughout the week by class teachers.
7.6. Regular checks will be carried out by staff and pupils (E-safety detectives) to monitor the uptake of E-safety policies.
7.7. E-safety will be integrated into PSHE and Computing units.
7.8. Through discussion, information, role play and 'what if?' situations, we hope to foster in our pupils a clear sense of how to make the right choices when it comes to digital technology.

8. Safeguards outside school

8.1. With increasing internet access and other digital advances at home, children will need to be as discerning about E-safety outside school as they would for, say, Stranger Danger. Parents will be shown the pupils' Acceptable Use agreement and to agree to Acceptable Use conditions for our pupils when at home. This includes supervising their children's use of the internet, the music they are accessing, images, video and text. It will be expected that a parent is aware of any communication between their child and other persons via the internet.
8.2. Parents will be recommended to follow E-safety guidelines at home:

- To check the histories and favourites of their child's browsing
- To place the computer in a communal area
- To be mindful of the amount of time their child spends on the computer
- To ensure that games, movies, images and music is all suitable for a child of primary school age
- To oversee any messaging, chat room or emailing their child is involved in.

8.3. Parents will be provided with information about E-safety in school meetings, and any concerns will be addressed by the computing co-ordinator.

9. How will incidents be handled?

9.1. The management of the Acceptable Use of the Internet in school is achieved by:

- Protection software installed on the network;
- Acceptable Use Policy adopted by the school;
- Staff contracts signed by all staff;
- A range of disciplinary procedures for infringements of the policy.

9.2. Whenever a student or staff member infringes the policy, the final decision on the level of sanction will be at the discretion of the school management.

10. Students

10.1. Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email

[Possible Sanctions – referred to class teacher]

10.2. Category B infringements

- Continual use of non-educational sites during lessons after being warned
- Unauthorised use of email after being warned
- Use of chatrooms or other contact sites

[Possible Sanctions – referred to the computing co-ordinator / removal of Internet access rights for a period]

10.3. Category C infringements

- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
- Transmission of commercial or advertising material
- Deliberately corrupting or destroying others' data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature
- Any purchasing or ordering of items over the internet

[Possible Sanctions – referred to computing co-ordinator / Headteacher / removal of Internet access rights for a period / possibly letter to parents]

10.4. Category D infringements

- Continued sending of emails regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion]

11. Staff

11.1. Category A infringements

- Excessive use of Internet for personal activities not related to professional development
- Excessive use of school digital resources for non-school use (printing photos, borrowing cameras, etc.)

[Sanction - referred to line manager]

11.2. Category B infringements

- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Endangering the school network by using unsafe materials (viruses, malware, spyware etc.)
- Bringing the school name into disrepute

[Sanction – Referred to Headteacher / disciplinary procedures]