St. Francis' Catholic Primary School

Online Safety Policy
March 2022

Approved by Governors: March 2022
Review date: March 2024

Mission Statement

Peace Love Knowledge

"As followers of Jesus and St Francis we pray that we are instruments of peace, learning to love And be loved, embracing our differences and Striving for excellence in all we do. Amen"

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Francis' Catholic Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St Francis' Catholic Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies (The Acceptable User Policy).
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

In addition to this, at St Francis' we believe learning about Online Safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life.

General

Our Online Safety policy has been written by the school, building on the London Grid For Learning (LGFL) exemplar policy and Local authority guidance.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive Online Safety education programme for pupils, staff and parents.

Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for Online Safety has been designated to the Designated Safeguard Lead who leads a team, which includes members of the senior management team.

Our school Computing Lead

Our Computing Leader ensures they keep up to date with Online Safety issues and guidance through liaison with the Local Authority Online Safety Officer and through organisations such as the London Grid For Learning (LGFL), The Child Exploitation and Online Protection (CEOP)[1] and the Local Authority. The school's Online Safety Lead ensures the Head, senior management and Governors are updated as necessary.

1

Governors need to have an understanding of Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of email;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, RM Unify, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- E-Bullying / Cyber bullying procedures/ peer on peer bullying online
- Their role in providing Online Safety education for pupils;
- Staff are reminded / updated about Online Safety matters at least once a year.

At St Francis', Online Safety is embedded in the curriculum to ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control (build on the knowledge, link actions and link learning online) and minimise online risks and how to report a problem.

We ensure that we engage with parents over Online Safety matters and that parents/carers have signed and returned an Online Safety Acceptable User Policy (AUP) form.

How we communicate with pupils on Online Safety.

- Online Safety is threaded throughout our Computing, RSHE. Citizenship and Anti-Bullying lessons. An Online Safety lesson is taught every half term and there is a module on Online Safety in Spring 1 for Years 1-6.
- Through activities and events during Safer Internet Week in February every year.
- Instruction in responsible and safe use precedes any lesson with Internet access.
- An Online Safety module is included in the Computing curriculum map covering both school and home use.
- Classes display Online Safety rules.
- Thinkuknow is on the RM Unify Launch Pad. This has a CEOP button to report online abuse. This can be accessed by staff, parents and pupils.

How we communicate with staff on Online Safety.

- Staff are aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff understand that online safety is a core part of safeguarding; as such it is part of everyone's job.
- Staff recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject.
- Staff are to read and follow this policy in conjunction with the school's main safeguarding policy
- Staff are asked to record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
-

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.
- Supply and temporary staff will be issued a login and asked to sign an AUP.
- A staff behaviour policy (called the code of conduct) includes: acceptable use of technologies, staff/pupil relationships and communications including the use of social media.

How we communicate with parents on Online Safety.

- A partnership approach with parents is encouraged. This includes parent meetings with demonstrations and suggestions for safe home Internet use.
- Internet issues are handled sensitively, and parents will be advised accordingly.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet are made available to parents.

What are the Online Safety issues?

Although the use of ICT and the Internet provide ever-increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

In past and potential future **remote learning and lockdowns,** there is a greater risk for exploitation and grooming as children spend more time at home and on devices.

Apart from the risk of children accessing Internet sites, which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.

At St Francis we create a safe learning environment, which means having effective arrangements in place to address a range of issues and we ensure that we have policies (Safeguarding, Child Protection, Anti bullying) and procedures in place, which are reviewed and adhered to by all staff, teaching and non-teaching whether in a paid or voluntary capacity.

How will complaints regarding Online Safety be handled?

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The Internet is managed via filtered access by LGFL and locally by RM. Children are trained how to act if they should access an unsuitable site or image. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions might be;

- Interview/counselling by class teacher / Online Safety Lead / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system.]
- Referral to the Police

Online Safety issues can be reported via a separate email.

Our Online Safety Lead acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with child protection procedures.

How we Manage Equipment and our ICT Infrastructure

At St Francis we:

- Ensure staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network login username and password and RM Unify login to access Google Classroom.
- Have a URL Filtering Platform to help protect pupils from accessing inappropriate websites on laptops, classroom computers or tablets.
- Provide pupils with an individual network login username and RM Unify login to access Google Classroom.
- Make it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Make clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Make clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Require all users to always log off when they have finished working or are leaving the computer unattended;
- Block all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblock other external social networking sites for specific purposes
- Work in partnership with RM to ensure that systems remain robust and protect students;
- Are vigilant in our supervision of pupils' use at all times, as far as is reasonable, and use common-sense strategies in learning resource areas;
- Ensure all staff and students have signed an acceptable user agreement form and understands that they must report any concerns;
- Require staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate websites;
- Plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Never allow a 'raw' image search with pupils e.g. Google image search;
- Inform all users that Internet use is monitored;
- Inform students that they must report any failure of the filtering systems directly to the class teacher. Class teachers should then contact the Online Safety Lead. Our system administrator then logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary.
- Immediately refer any material we suspect is illegal to the appropriate authorities and the Police.
- Follow the guidance of the LGFL use of digital and video images policy.
- Follow the guidance of the LGFL acceptable use of the Internet and related technologies.
- Follow the guidance of the LGFL on the use of AUPs in KS1 and KS2
- Follow the guidance of the LGFL on Online Safety for Parents/carers
- Follow the guidance of the LGFL on e- safety for staff and adults working with children.
- Members of staff are able to use the school Wi-Fi by signing in with their LGFL username and password. Restrictions and website filtering is still applied when personal devices are signed in to the school's Wi-Fi.

School website

- The Head Teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, info@st-francis.newham.sch.uk. Home information or individual email identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded data in respect of stored images

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- School staff will ensure that in private use:
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Radicalisation and our Prevent Duty

- The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content and social media.
- Where staff, students or visitors find unblocked extremist content they must report it to our school's single point of contact in relation to Prevent.