St Francis Catholic

Primary School

Online Safety Policy

Head Teacher **Mrs Dawn Richards**

Chair of Governors **Mr Peter Gough**

Date written **Autumn 2023**

This policy will be reviewed on an annual basis unless circumstances require policy update in the interim.

School Mission Statement

'I am a sign of God's love'

At St Francis we love, learn and grow in the footsteps of Jesus and are active signs of God's love through praying, respecting and serving others.

STATEMENT OF INTENT

At St Francis Catholic Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. LEGAL FRAMEWORK

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

1.2. This policy also has regard to the following statutory guidance:

- DfE (2023) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Computing and ICT Policy
- Social Media Policy
- Safeguarding Policy
- Acceptable Use Policy for adults and children in school
- Mobile device Policy

2. USE OF THE INTERNET

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

2.4. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Online safety is considered whilst planning the whole curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

3. ROLES AND RESPONSIBILITIES

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. The **Safeguarding team** is responsible for ensuring the day-to-day Online Safety in the school, and managing any issues that may arise. Smoothwall filters and monitors all online use on the school network, creating weekly reports which are sent to DSL and any miss-use is reported to the Head Teacher.

3.4. The **Head Teacher** is responsible for ensuring that all staff receives CPD to allow them to fulfil their role.

3.5. The **DSL and Computing Lead** will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo annual updated safeguarding training and be able to teach pupils about online safety.

3.6. The **Computing Lead, ICT Technician and DSL** will regularly monitor the provision of Online Safety in the school and will provide feedback to the **Head Teacher**.

3.7. A log will be kept of all submitted Online Safety reports and incidents.

3.8. All incidents of inappropriate internet use must be logged on CPOM's immediately if a child or reported to the **Head Teacher** if an adult.

3.9. The **Safeguarding Team** will ensure that all members of staff are aware of the procedure when reporting Online Safety incidents, and will keep a log of all incidents recorded on CPOM's. Information of Smoothwall records are kept online.

3.10. The **Safeguarding Team** will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school. (See Safer Recruitment Policy)

3.11. Cyber bullying incidents will be reported in accordance with the school's **Acceptable Use Policy, Code of Conduct, and Behaviour Policy.**

3.12. The **Governing Body** will evaluate and review this Online Safety Policy on a yearly basis, taking into account the latest developments in ICT and the feedback from staff and pupils.

3.13. The **Head Teacher** will review and amend this policy with the **Safeguarding Team**, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.14. Teachers are responsible for ensuring that Online Safety issues are embedded in the curriculum and safe internet access is promoted **at all times**.

3.15. All staff are responsible for ensuring they are up-to-date with current Online Safety issues, and this Online Safety Policy.

3.16. All staff and pupils will ensure they understand and adhere to our **Acceptable Use Agreement**, accepting each time they log on to the school network.

3.17. The **DSL and Computing Lead** are responsible for communicating with parents regularly and updating them on current Online Safety issues and control measures.

3.18. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. ONLINE SAFETY EDUCATION

4.1. Educating pupils:

- An Online Safety programme, Google Smart – Be Internet Legends, Ten:Ten, MrPICT and National Online Safety Resources, will be used and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of technology both inside and outside of the school.
- Pupils will be taught about the importance of Online Safety and are encouraged to be critically aware of the content they access online, and the validity of website content.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.

4.2. Clear guidance on the rules of internet use will be presented on all computers in school. When logging onto a computer all children and staff must accept the acceptable use policy.

4.3. Pupils are instructed to report any suspicious use of the internet and digital devices. When there is 'something wrong' with the content, children are taught to turn monitors off and alert an adult.

4.4. Lessons will be used to educate pupils about cyber bullying, in line with the RSE curriculum and policy, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

4.5. The school will hold Online Safety events, such as Safer Internet Day and assemblies throughout the year to promote Online Safety.

4.6. Educating staff: All staff will undergo Online Safety Training annually and any updates in Staff Briefing to ensure they are aware of current Online Safety issues and any changes to the provision of Online Safety, as well as current developments in social media and the internet as a whole.

All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo Online Safety training as part of their induction programme, ensuring they fully understand this Online Safety Policy.

4.7 The **DSL and Computing Lead** will act as the first points of contact for staff requiring Online Safety advice.

4.8. Educating parents:

- Online Safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and workshops.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any Online Safety related concerns.

5. ONLINE SAFETY CONTROL MEASURES

5.1. To access the school network, including the internet, all users must accept the **Acceptable Use Agreement** which forms part of the 'logging on' process on all devices within the school.

5.2. All users in **Key Stage 1 and 2** will be provided with usernames and are advised to keep these confidential to avoid any other pupils using their login details.

5.3. Pupils' computer activity is continuously monitored by Policy Central the forensic monitoring software.

5.4. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.5. The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

5.6. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by **the Head Teacher.**

5.7. All school systems will be protected by up-to-date virus software.

5.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

5.9. Master users' passwords will be available to the **Head Teacher** should they need to monitor use.

5.10. Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from using any personal devices.

Email:

5.11. Staff will be given approved email accounts and are only able to use these accounts for any school related emails.

5.12. The use of personal email accounts to send and receive personal data or information is not permitted; staff must adhere to the rules of the Acceptable Use Policy.

5.13. No sensitive personal data shall be sent to any other staff or third parties via email.

5.14. Staff members are aware that their email messages can be monitored.

5.15. Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Social networking:

5.16. Use of social media on behalf of the school will be conducted following the processes outlined in our **Social Media Policy**.

5.17. Access to social networking sites will be filtered as appropriate.

5.18. Pupils are regularly educated on the implications of posting personal data online outside of the school.

5.19. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

5.20. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

5.21. Staff are not permitted to publish comments about the school which may affect its reputability.

5.22. Staff are not permitted to access personal social media sites during teaching hours unless it is justified to be beneficial to the material being taught.

Published content on the school website and images:

5.23. The **Head Teacher** will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.

5.24. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

5.25. Images and names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received for each academic year.

5.26. Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment without permission from the Head Teacher.

5.27. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

5.28. Mobile devices are not permitted to be used during school hours by pupils, pupils are requested to not bring devices into school.

5.29. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the monitoring software.

5.30. The sending of inappropriate messages or images from mobile devices is prohibited.

5.31. The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5.32. Staff are permitted to use personal mobile devices in the staffroom only.

5.33. Staff are permitted to wear Smart Watches, although these must be set to silent and notifications turned off. No calls are to be taken or messages read/ replied while in the vicinity of children.

5.34. **Network security:**

- Network profiles for each pupil are created, in which the individual must enter a username when accessing the ICT systems within the school.
- Network profiles for each staff member are created, in which the individual must enter a username when accessing the ICT systems within the school.
- Passwords should be stored using non-reversible encryption.

5.35. **Virus management:** Symantec Virus protection is supplied and monitored by the LA ICT Services.

6. CYBER BULLYING

6.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

6.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

6.3. The school will regularly educate staff, pupils and parents on the importance of staying safe Online, as well as being considerate to what they post online.

6.4. Pupils will be educated about Online Safety through teaching and learning opportunities as part of the RSE curriculum, computing curriculum and other appropriate times throughout the wider curriculum.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with **Behaviour Policy.**

7. REPORTING MISUSE

- **St Francis Catholic Primary School** will clearly define what is classed as inappropriate behaviour in the **Acceptable Use Agreement**, ensuring all pupils and staff members are aware of what behaviour is expected of them.
- Inappropriate activities are discussed and the reasoning behind prohibiting activities due to Online Safety are explained to pupils as part of the curriculum in order to promote responsible internet use.
- **Misuse by pupils: See response to incident of concern flowchart**
- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.

- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the DSL via CPOMs.
- Parents of any pupil who does not adhere to the rules outlined in our **Acceptable Use Policy** will be informed if they are found to be wilfully misusing equipment, the network or the internet.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material or sexting, shall be dealt with in accordance with our **Child Protection and Safeguarding Policy**.

7.1**Misuse by staff:** Any misuse of the internet by a member of staff should be immediately reported to the **Head Teacher**. The Head Teacher will deal with such incidents and may decide to take disciplinary action against the member of staff.

- The **Head Teacher** will decide whether it is appropriate to notify the police or appropriate officers in the Local Authority of the action taken against a member of staff. The chair of governors will be informed of any notifications.

7.2. **Use of illegal material:**

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the **DSL** and **Head Teacher** will be informed and the police contacted.
-

8. MONITORING AND REVIEW

- Evaluation and review of this Online Safety Policy will take place on a yearly basis, taking into account the latest developments in ICT and the feedback from staff/pupils; any changes made to this policy will be communicated to all members of staff.

Flowchart for reporting an incident: