St Mary's Catholic High School

E-Safety Policy

Created: June 2015 Reviewed: November 2019 Review by: September 2021

Statement of Intent

This policy has been updated in line with the requirements of the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, to include further information on consent, data security and the responsibilities of the data protection officer (DPO). The updated policy also includes reference to the 2018 version of Keeping Children Safe in Education.
Elements added or updated in response to the regulations have been highlighted as appropriate, e.g. **[New]** or **[Updated]**.

At St Mary's Catholic High 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 mitigate the risk of harm.

1. Legal Framework

1.1. This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation
- Freedom of Information Act 2000

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

- DfE (2018) 'Keeping children safe in education'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'

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

- **E-security Policy**
- **Digital Safeguarding Policy**
- **Cyber Bullying Policy**
- **Social Media Policy**
- **Allegations of Abuse Against Staff Policy**
- **Acceptable Use Agreement**
- **Data Security Breach Prevention and Management Plan**

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 the following:

- 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. content involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

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 E-Safety Officer, Mr D. Orme, is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

3.4 The headteacher is responsible for ensuring that the E-Safety Officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.6 The E-Safety Officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.7 The headteacher and data protection officer (DPO) will ensure there is a system in place which monitors and supports the E-Safety Officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.8 The E-Safety Officer will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.9 The headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.10 The E-Safety Officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

3.11 The e-safety officer 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.

3.12 The governing body will request regular information from with the E-Safety Officer on the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.13 The governing body will evaluate and review this E-safety Policy on a bi-annual basis, considering the latest developments in ICT and the feedback from staff/pupils.

3.14 The headteacher will review and amend this policy with the E-Safety Officer and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.15 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.16 All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.17 All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the headteacher.

3.18 Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.19 The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

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

4. E-Safety Education

Educating pupils:

4.1 An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

4.2 Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.

4.3 Pupils will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.

4.4 Clear guidance on the rules of internet use will be presented in all classrooms.

4.5 Pupils are instructed to report any suspicious use of the internet and digital devices to their classroom teacher.

4.6 PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

4.7 The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

Educating staff:

4.8 A planned calendar programme of e-safety training opportunities is available to all staff members, including whole school activities and CPD training courses.

4.9 All staff will undergo e-safety training on a termly basis to ensure they are aware of current e-safety issues and any changes to the provision of e-

safety, as well as current developments in social media and the internet as a whole.

4.10 All staff will undergo regular audits by the E-Safety Officer in order to identify areas of training need.

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

4.12 All staff will be educated on which sites are deemed appropriate and inappropriate.

4.13 All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.14 Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.15 The E-Safety Officer will act as the first point of contact for staff requiring e-safety advice.

Educating parents:

4.16 E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

4.17 Twilight courses and presentations may be run by the school for parents.

4.18 Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-Safety Control Measures

Internet access:

5.1 Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

5.2 Where a pupil is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify parents that the pupil has consented independently.

5.3 A record will be kept by the school office of all pupils who have been granted internet access.

5.4 All pupils will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

5.5 Pupils' activity is continuously checked by Lanschool monitoring software.

5.6 Management systems are in place (Lanschool) to allow teachers and members of staff to control workstations and monitor pupils' activity.

5.7 Effective filtering systems are in place to mitigate any potential risks to pupils attempting to access websites containing harmful or inappropriate material.

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

5.9 Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the E-Safety Officer.

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

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

5.12 System access will be available to the headteacher for regular monitoring of activity.

5.13 Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

5.14 Personal use will only be monitored by the E-Safety Officer for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

5.15 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. This will be dealt with following the process outlined in the misuse by staff section of this policy.

Email:

5.16 Pupils and staff will be given approved email accounts and these must be used for school business only.

5.17 The use of personal email for school use is prohibited.

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

5.19 All email messages are monitored and the filtering system will detect and flag inappropriate links, viruses, malware and profanity to the E-Safety Officer.

5.20 Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

5.21 All malicious emails will be deleted automatically.

5.22 The E-Safety Officer will, at the start of each school year, brief the staff on E-Safety issues.

5.23 Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The E-Safety Officer will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

5.24 The use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.

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

5.26 Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.

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

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

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

5.30 Staff are not permitted to publish comments about the school which may affect its reputation.

5.31 Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

Published content on the school website:

5.32 The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

5.33 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.

5.34 Images and full 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.

5.35 Pupils are not permitted to take or publish photos of others without permission from the individual.

5.36 Staff are able to take pictures, though they must do so in accordance with our Photography Policy. Staff will not take pictures using their personal equipment, unless approval from the Headteacher is granted.

5.37 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:

5.38 The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

5.39 Pupils are not permitted to access the school's Wi-Fi system at any time using their mobile devices and hand-held computers.

5.40 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 E-Safety Officer where it is justifiable to do so and the justification outweighs the need for privacy.

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

5.42 The DPO will, in collaboration with the E-Safety Officer ensure all school-owned devices are password protected – these passwords will be changed on a regular basis to ensure their security.

5.43 Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Network security:

5.44 Network profiles for each pupil and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.

5.45 Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.

5.46 Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.

5.47 Passwords will be required to change termly to ensure maximum security for staff accounts.

5.48 Passwords should be stored using non-reversible encryption.

5.49 The following passwords will not be accepted by the school's security systems as they are too predictable:

- Password
- Pa55word
- Password123
- Qwerty
- 123456
- 12345678
- ABC123

5.50 The E-Safety Officer will ensure all school-owned laptops and computers have their encryption settings turned on and are protected with Sophos InterceptX.

5.51 Important folders and systems, e.g. those including pupils' medical records, will be restricted by group policy and/or username & password so only permitted staff have access to ensure their security.

Virus management:

5.52 Technical security features, such as virus software, are kept up-to-date and managed by the E-Safety Officer

5.53 The E-Safety Officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.54 The Firewall is switched on at all times. Updates are applied automatically by the Sophos UTM. Staff must restart their computers as soon as possible when prompted by the system to do so following an update.

5.55 Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's Data Security Breach Prevention and Management Plan.

5.56 Staff members will report all malware and virus attacks to the E-Safety Officer and DPO immediately.

E-safety committee:

5.57 The E-safety Policy will be monitored and evaluated by the Governor's Resources committee on a termly basis.

6. Cyber Bullying

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

6.2 The school recognises that both staff and pupils may experience cyber bullying and is committed to responding appropriately to 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 a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

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 utmost seriousness and will be dealt with in accordance with our Anti-Bullying and Harassment Policy and Cyber Bullying Policy.

6.7 The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

7. Reporting Misuse

7.1 St Mary's Catholic High 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.

7.2 Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

7.3 Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.

7.4 Any instances of computer misuse should be immediately reported to the E-Safety Officer, who will then report this to the headteacher using a complaints form.

7.5 Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet will have a letter sent to their parents explaining the reason for suspending their internet use.

7.6 Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.

7.7 Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

Misuse by staff:

7.8 Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a complaints form.

7.9 The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy and may decide to take disciplinary action against the member of staff.

7.10 The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Use of illegal material:

7.11 In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

7.12 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.

7.13 If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.

7.14 Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.