English Martyrs Catholic Primary School

"where everyone is special"

P57: Online Safety Policy

Mission Statement
With Christ at the heart of our Catholic community, our mission is to: ✠ nurture the potential in each individual, ✠ celebrate achievement, ✠ and develop an awareness of service to God and each other

Adopted by the school: November 2020

Review: When required

1. Purpose of Online Safety Policy

This Online Safety Policy has been created by English Martyrs Catholic Primary School Teachers, Governors and School Councillors.

The aim of the policy is to provide students, parents and staff with information on how the school will;

- Safeguard and protect students, staff and parents/carers.
- Educate and raise awareness of online safety throughout the school and local community.
- Manage professional standards and practice when using technology.
- Identify clear procedures when responding to online safety concerns.

Although considerable, the school outlines 3 significant areas of risk.

1) Content – Being exposed to illegal/ inappropriate materials.
2) Contact – Being exposed to, and exposing others to, harmful online interaction.
3) Conduct – Personal online behaviour which could lead to harm.

2. Why Internet use is important

- Internet access is an entitlement for pupils.
- Technology (computers, tablets, phones) is an important part of everyday life and should be taught to develop a range of strategies to respond to risk online.
- Online safety issues are embedded in all aspects of the curriculum. During Computing sessions, teachers reference Online Safety where appropriate.

3. Writing and reviewing the Online Safety Policy

- The Online Safety Policy has been written by the Online Safety Coordinator in conjunction with Governors and Head Teacher.
- The Online Safety Policy will be reviewed annually and compliance will be monitored throughout the year by the Head teacher, Senior Leadership team and Online Safety Lead.
- The Online Safety Policy will be read, reviewed and signed by Class Teachers annually or after any serious incident.

4. Roles and Responsibilities

4.1 Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- A member of the Governing Body will attend Online Safety meetings and report back to other Governors and attend relevant training.

4.2 Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online safety will be delegated to the Online Safety Co-coordinator where appropriate.
- The Head teacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online safety roles and to train other colleagues.

4.3 Online Safety Coordinator

• Leads Online Safety Group

• Overall day to day responsibility. Online Safeguarding is discussed with the DSL lead and a plan of action is set up on an individual basis.

• Annual training for Staff and parents.

• To review the Online Safety Policy with other relevant members of staff yearly or after any serious incident - ensuring the effectiveness.

• Keep up to date with new risks, issues, developments and resources in the area of online safety

4.4 Teaching and Support Staff:

• Read, understand and sign the school Staff Acceptable Use Policy / Agreement.

• Report any suspected misuse or problem to the Online Safety Coordinator / Head teacher (and designated safeguarding lead) for investigation / action / sanction.

• Have an up to date awareness of online safety.

• Staff monitor ICT activity in lessons, extra-curricular and extended school activities.

4.5 Pupils:

• Are responsible for using the school ICT systems in accordance with the Acceptable Use Agreement (Appendix 2 and 3) which they will be expected to sign before being given access to school systems.

• Should use their own user ID and password as appropriate.

4.6 Student Voice – School Councillors/Digital Leaders

• Feedback on current concerns or online interests.

• Lead class session on Online Safety once a term (lesson will be planned during a school council session).

4.7 Parents / Carers:

• Parents/Carers will have the opportunity to attend an Online Safety workshop - date arranged and led by the Online Safety Coordinator.

5. <u>Infrastructure, system security, filtering and monitoring</u>

• The Online Safety Policy will be reviewed annually, after any serious incident or after any local/national policy requirements.

• Virus protection will be installed and updated after serious incidents.

• The school will work in partnership with the Warwickshire ICT Development Service for filtering and monitoring. All, possible harmful reports will be highlighted to the Online Safety Lead.

• If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Online Safety Lead, who will report this to the ICT Development Service filtering team and block it.

5.1 Usernames and passwords

• All pupils will be provided with a username and password in order to secure safe access to school curriculum devices, the Learning Platform and email. Pupils must use these when accessing school equipment.

• Students will be made aware that all technology will be monitored and be traced back to the individual user.

• Staff should never use a class log on for their own network access.

Staff must

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Transfer data using encryption and secure password protected devices.

5.2 All Staff will be provided with a username and password which will provide them secure access to school curriculum devices, the Learning Platform and email.

• Staff are provided with a username and password through the Warwickshire Learning Platform. Staff must use these when accessing school technology.

• Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

• 'Guests' such as supply teachers are provided with a username and password if they require access to school systems.

• Staff will be made aware that all online use is monitored and understand the implications of misuse in line with the Acceptable Use Policy.

5.3 Authorising Internet access

• All staff must read and sign the school Acceptable Use Policy, before using any school ICT resource.

• Parents will be asked to sign and return a consent form in Reception or when a new student is registered. 5.4 Assessing risks

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

• In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.

5.4 Curriculum

• Online safety should be a focus in all areas of the curriculum and staff should, where appropriate, reinforce online safety messages.

• Pupils will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

• Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5.5 Data Protection

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

Staff responsibilities

1) Ensure the safe keeping of personal data.

2) Ensure that they use secure, school technology and are securely logging off after each use.

5.7 When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.

5.8 Publishing and storing pupil's images

- Photographs that include pupils will be selected carefully, and photographs of individual pupils will only be taken when relevant to particular events, activities or lessons.
- Pupils' full names will not be used anywhere on the Website, learning platform, on school Social Media pages or stored within folders in the 'shared' or 'pupil shared' areas

6. **<u>Communications</u>**

6.1 Email

- Pupils may only use approved We-Learn Email accounts on the school system. These may only be accessed through the School Learning Platform.
- Pupils are taught not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

6.2 Social networking and personal publishing

- Pupils are taught about the safe use of social networking sites as part of their online safety lessons.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Any contact made by a stranger is turned off and reported to a parent, teacher or adult of trust.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils, and that many social networking sites have a specified minimum age.

6.3 Learning Platforms, Virtual Learning Environments and other communication tools

- Pupils will be taught how to use communication tools appropriately, as part of general ICT lessons and online safety lessons.
- Pupils/staff will be advised on acceptable conduct and use when using communication tools.
- All users will be mindful of copyright issues and will only upload appropriate content.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

6.4 Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- Access to the communication tool for the user may be suspended period of time.
- The user will need to discuss the issues with a member of SLT before being permitted to use school technology again.

- A pupil's parent/carer may be informed.

6.5 Mobile Phones & Tablets

- Pupils are not allowed access to mobile phones or tablets into school. If they need to bring them to school they must be handed in at the school office on entering school and collected at the end of the school day.
- Mobile phones or personal tablets will not be used by staff during face-to-face sessions with pupils.
- Staff mobile phones should not be accessible by pupils.
- Staff will be made aware that connecting a personal mobile phone / Smart phone to the school's wireless system will result in that phone being monitored in the same way that networked devices are monitored.

7. 'Sexting and Sexual Imagery'

7.1 If the school is made aware of any incident involving sexting/sexual images involving a child we will;

Act in accordance with our Child protection and Safeguarding policies and work closely with the police/local authority.

- Store the device securely.
- Immediately notify the DSL and Online Safety Lead.
- If an indecent image has been shared on the Learning Platform, all online access to will be blocked to users (students and staff) and isolate the image.
- Carry out a risk assessment which considers any vulnerable students involved; including carrying out relevant checks with other agencies.
- Inform parents at an early stage, if appropriate, about the incident and how it is being managed.
- Make a referral to Specialist Children's Services/Police.

7.2 If a decision is made to view imagery the DSL's would need to be satisfied that viewing:

- Is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report
- Is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network.

7.3 If it is necessary to view the imagery then the DSL's should:

- Never copy, print, save or share the imagery.
- Ensure viewing is undertaken by the DSL with at least 1 other member of the SLT.
- Ensure viewing takes place with another member of staff present in the room, ideally the Headteacher or a member of the senior leadership team. This staff member does not need to view the images.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the image.
- Keep a record of the viewing in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions. (Appendix 1)
- Ensure the record keeping is signed, dated and meets the wider standards set out by Ofsted for recording safeguarding incidents. After every sexting or sexual image incident

- Images will be deleted only once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized, a teacher who has been formally authorised by the Headteacher can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone. If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved

---

After every incident

The SLT and Online Safety Lead will review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

8. Recording incidents

8.1 All incidents relating to youth produced sexual imagery need to be recorded in school.

This includes incidents that have been referred to external agencies and those that have not.

8.2 Staff at English Martyrs Catholic Primary School will record incidents in line with the above guidance.

Where we decide not to refer incidents to the police or children's social care, we will record the reason for doing so and ensure that this is signed off by the Head Teacher.

9. Complaints and misuse.

- Complaints of Internet misuse will be dealt with by the Head teacher.
- If any apparent or actual misuse appears to involve illegal activity i.e. Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials
- The school will report the incident to the Local Authority in the first instance and inform the police.

9.2 **Staff should refer to the 'Whistle Blowing policy' should they have complaints about a senior member of staff's use of the internet and feel they cannot approach the Head teacher.**

This can be found in the policies folders, staff room or online.

9.3 Inappropriate usage by Pupils includes:

- Deliberately accessing or trying to access material that could be considered illegal
- Deliberately accessing or trying to access material that is not age-appropriate
- Unauthorized use of non-educational sites during lessons
- Attempting to access or accessing the school network / Learning Platform using another users account.
- Sending an email, text or other electronic message that is regarded as offensive, harassment or of a bullying nature.
- Actions which could bring the school into disrepute or breach the integrity or ethos of the school.

9.4 **Staff, will in line with the 'Behaviour Policy', will use one or more of the following sanctions depending on the severity of the misuse**.

- Verbal.
- Refer to the Online Safety Coordinator.
- Refer to the Head Teacher.
- Inform parents / carers.
- Remove network / internet access rights.
- Refer to the police.

9.5 Inappropriate usage by Staff

Staff misuse of technology/internet is outlined in the school Code of Practice Staff Policy.

9.6 Depending on the serious of the inappropriate use by a member of staff, the Online Safety Lead / Headteacher may use one or more of the following sanctions:

- Refer to the Local Authority / ICT Development Service or HR.
- Refer to Technical Support staff for action re: filtering.
- Disciplinary action.
- Refer to the police.

9.7 Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated at English Martyrs Catholic Primary School
- All incidents of Cyberbullying reported to the school will be recorded along with the response and outcome.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- All reported cases of cyberbullying will be recorded and investigated by the Online Safety Lead and/or Head teacher.

9.8 Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers, from both parties, will be informed.
- The Police will be contacted if a criminal offence is suspected.
- Ultimately a child could be excluded in line with the behaviour policy.

10 Preventing extremism and radicalisation

We know that extremists use the internet, including social media to share their messages. The filtering systems used at school block inappropriate content, including extremist content.

Where staff, pupils or visitors find unblocked extremist content they must report to the online safety coordinator or ICT coordinator and Head teacher immediately – resulting in an immediate block of the website and a report being given to appropriate authorities. If a pupil is found to be actively searching for extremis content the DSL's must be informed so that they can take the appropriate action

11 Using social media to engage/update parents and families

At English Martyrs Catholic Primary School, we aim to use as many different ways as possible including Facebook, Twitter to keep our parents and families up to date with what their children are doing and what is going on in school.
In line with the Online policy:

- Access will be password protected.
- Only the operating Class Teacher/LSA's will have access and must use a school, password protected, equipment.
- Pupils, parents and visitors of English Martyrs will not have access to class pages of other classes.

English Martyrs Catholic Primary School

Appendix 1

Part 1

Youth produced Sexual Imagery

Incidents Recording Sheet

Date:	Time imagery declared/discovered:
Adults involved:	Children involved:

Time Reported to:

DSL:

Head:

Online Safety Lead:

Details of imagery:

Next steps/ agencies reported to	Adults involved from school and agencies

Outcomes- any changes to be made to policy/staff training and adults that will monitor this

Part 2

Who initially decided the imagery need to be viewed or deleted?	
Which adults were involved in this decision? DSL Headteacher Senior leaders	
Why was the decision to view/delete taken? Please add as much detail as possible.	
Which adult viewed/deleted the imagery? When possible a same sex adult should view imagery.	
In which room did this take place? And with which adults in the same room at the time of viewing/deletion?	

Please complete Part 1 and make sure the outcome in Part 2 is recorded.