Policy written –September 2024

Date approved by the full Governing body-

October 2025

Review September 2026

St Mary's Catholic Primary School

E-SAFETY POLICY

School Mission Statement

Loved and inspired by Mary, we shine and learn as a family of God.

School Policy

The school has computers, ipads and Internet access to help learning. On the internet there is a huge wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. At St Mary's we believe that the pupils should have opportunity to use these resources to support their learning. VirtualLearning Environments (VLEs) such as Purple Mash provide children and/or young adults with a platform for personalised and independent learning. There are many advantages to effective use of technology such as-

- Children and/or young adults are equipped with skills for the future.
- The Internet provides Instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's reading and research skills.
- Email, instant messaging and social networking helps to foster and develop good social and communication skills.

Therefore, at St Mary's we will ensure that children have the opportunity to benefit from the use of ICT in a safe and responsible way. We will also ensure that children learn the correct way to conduct themselves online as well as what to do should breaches of security occur.

Safety

The Internet provides access to a greater library of resources to support learning. However, where as, the resources in school are carefully selected to be consistent with national and school policies those on the Internet are not. Therefore the school will only connect to the Internet through the Lancsngfl site. A service provider that is monitored and regulated to allow material that has been deemed suitable for children to be viewed. Children will only be allowed to use the Internet when there is adult supervision. The positive use of the internet as a learning resource far outweighs the risks involved. The children will be taught about the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

Rules for the safe use of the Internet have been established. These rules will be discussed with the pupils and also displayed near Internet access for referral. All children will also sign up to an acceptable use policy which will outline the behaviour expected whilst online.

Parental approval

All parents are asked for permission for the acceptance of their child using the school internet service. Attention is drawn to it being a valuable learning aid, and that there are great restrictions to the level of information accessible.

Procedures for Use of our Network

- Users must respect confidentiality and attempts should not be made to access another individual's login on the network without permission.
- Software should not be installed without prior permission from the ICT Co-ordinator.
- Permission to use removable media (e.g. pen drives / memory sticks) must be given by the class teacher.

Procedures for Use of the Internet and Email

- Parental consent is requested to allow internet access in school. All pupils are aware of the Rules for responsible Internet Use.
- All teachers in our school have access to the Office 365 e-mail system.
- Only official email addresses are used to contact staff/pupils.
- The Internet and email must only be used by pupils for educational purposes.
- Children must be supervised at all times when using the Internet and email.
- All users must immediately report any mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the E-safety co-ordinator. In the event of access turn **off** the monitor **not** the PC and contact the E-safety co-ordinator who will then make a note of the offending website address (URL) taken so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- Email will be taught through using purple mash, a closed virtual learning service where children can only send emails internally which are seen by the teachers.

- Children will be taught the importance of not disclosing any information of a personal
nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions,
appropriate to the case, will be imposed on any users who break this code.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

Procedures for Use of Instant Messaging (IM), Chat and social media sites.

- The use of Instant messaging (e.g. MSN messenger) is not permitted
- Use of social-networking websites (e.g. Bebo, MySpace, Facebook, Habbo, Piczo, etc.) is not permitted.
- Children/Young adults and staff must not access public or unregulated chat rooms.
- Adults in school are not permitted to add pupils or past pupils as 'friends' on Social Media Sites.
- All social media and instant messaging sites are blocked in school.

Procedures for Use of Cameras, Video Equipment and Webcams

- Permission must be obtained from a child's parent or carer before photographs or video footage can be taken.
- Only school equipment will be used to record images either in school or during a trip or visit. Personal equipment is **not** to be used.
- Webcams must not be used for personal communication and should only be used with an adult present in specific computing lessons.
- Children / Young adults and staff must conduct themselves in a polite and respectful manner when representing the establishment/service in a video

conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of the School website/VLE

- The website administrator/head teacher is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school website is subject to frequent checks to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.
- Copyright and intellectual property rights must be respected.
- Permission will be obtained from parents or carers before any images of children are uploaded onto the School website.
- Names must not be used to identify individuals portrayed in images uploaded onto the School website. Similarly, if a child / young person or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Procedures for using mobile phones, Ipads, smart watches, air tags and equivalent tracking devices.

- Children are not permitted to bring mobile phones/ ipads into school. In exceptional circumstances a parent can request that their child has a mobile phone for use after school. This phone will be kept in the office for the child to receive at the end of the day. The phone will be switched off at all times whilst on school premises.

• Pupils are not permitted to wear, carry, or bring Mobile Phones, Smart Watches, AirTags or any other electronic tracking devices into school.

• Tracking devices can cause unnecessary upset or confusion if activated during the school day.

• Smart watches, due to their features such as online accessibility, recording and capturing facilities can create potential safeguarding and distraction issues.

• The school has robust safeguarding and supervision procedures in place. Parents and carers are asked to place their trust in staff to keep children safe while in our care.

• Any device brought into school will be removed from the pupil's possession, stored securely by staff, and returned to parents/carers at the end of the day.

- Staff are permitted to bring mobile phones but they must be switched off whilst in school. Any phone calls will need to be taken at designated break times away from the children. In the event of an urgent phone call needing to be made a request will be made to the headteacher.

- Volunteers and parents will be asked to turn off their mobile phone upon entry to the school. Parents will be asked (via the school newsletter) to be mindful on not taking pictures whilst on the playground at pick up and drop off times.

- Pictures taken of children will always be done on school ipads or cameras. Pictures will never be taken on personal devices. Once taken the pictures may be downloaded for use on school computers. At the end of each year the photographs stored on the school ipads will be deleted.

Rationale

• Safeguarding: These devices can inadvertently compromise safeguarding arrangements by: Giving inaccurate or misleading location information, Devices with internet access, cameras, and messaging functions can pose risks to children's safety and wellbeing, including exposure to inappropriate content, cyberbullying, or unwanted contact.

• Disruption to Learning: Phones and smartwatches can distract pupils from their lessons and reduce focus on learning and play.

• Wellbeing: Alerts or notifications received during the school day may cause unnecessary worry or distress to pupils, parents, or staff.

• Privacy: The use of tracking devices, cameras or recording functions could compromise the privacy of both pupils and staff.

• Trust: The school is responsible for pupils' safety during school hours and activities. Confidence in these procedures is essential.

Sanctions to be imposed if procedures are not followed

- Parents or carers will be informed of any malpractice.
- Users may be suspended from using the school computers, Internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

Concluding Statement

This policy will be checked and updated annually. It may be that staff / children might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon approval by the head teacher and governing body, which will be used to inform future policy updates

Other Policies that have relevance to internet safety

- Safeguarding/Child Protection
- Acceptable use policy