St Mary's Catholic Primary School

At St Mary's we live and learn sharing God's love

E-Safety

Table of Contents

Introduction

This E-safety policy has been written by the school, building on the Lancashire County Council and Government guidance. The policy has been agreed by the senior management and adopted by the Governing body. This policy will be reviewed and updated accordingly on an annual basis.

St. Mary's vision for E-safety:

There are many benefits and opportunities the internet has to offer as a means of enhancing learning. However, as a school, we have a duty of care in ensuring our pupils are safe in their use of the internet. At St. Mary's, we treat E-safety as a whole school community issue.

E-safety depends on staff, governors, parents and pupils taking responsibility for the safe use of the internet.

To equip our pupils with the necessary knowledge and understanding, we embed the teaching of E-safety within the computing curriculum. Furthermore, staff reiterate E-safety guidance during the wider curriculum when accessing the internet and expand on issues during E-safety days that take place during the school year. E-safety displays can be found around the school outlining our E-safety rules.

As a school, we also aim to work closely with parents/carers to ensure that the school's E-safety ethos and approach are shared. We try to ensure parents understand E-safety issues, risks and their roles and responsibilities. To achieve this, we have a designated section on our school website with links to appropriate resources and guidance. In addition to this, we pass on up to date information via newsletters and offer planned parent/carer workshops and open days.

The school's E-safety Champion

The school's E-safety Champion is Mrs O'Mahony and she is the main point of contact for E-safety related issues and incidents. Mrs O'Mahony will work closely with the DSL team as necessary.

The role of the E-safety Champion:

- Having operational responsibility for ensuring the development, maintenance and review of the school's E-safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an E-safety incident occur.
- Ensuring an E-safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with E-safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging E-safety advice/training for staff, parents/carers and governors.
- Ensuring the Head teacher, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Leads to ensure a co-ordinated approach across relevant safeguarding areas.

Security and data management

Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR. Data should be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

- Only transferred to others with adequate protection.

At all times staff must ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Personal data should only be used on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data. Data should only be transferred using encryption and secure password protected devices.

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

- data must be encrypted and password protected
- device must be password protected
- device must offer approved virus and malware checking software
- data must be securely deleted from the device once it has been transferred or its use is complete.

Photographs

Images of children and personal data should not be stored on personal phones, cameras, tablets, laptops, PC's or removable storage devices. Staff are not permitted to take home school equipment that has photographs of pupils (past or present). All school devices are password protected. Photographs will be held on the school's server for one academic year. Images will be deleted from portable equipment such as iPads at the end of each term. Photographs relating to school pupils will be stored in a secure area on OneDrive in the "Photographs Folder". The folder will be named "Academic Year <>" to allow for optimal management of the data.

Use of mobile devices

iPads

School has a number of iPads for staff and pupil use. These should be used for educational purposes only. Children need to be taught responsible use of these devices including; access to the internet, photographing and recording other pupils or themselves and how to store data safely.

Mobile Phones

Children are not allowed to have mobile phones with them in school. We accept that mobile phones are widely owned by children of all ages. However, if they are brought into school, they must be handed in straight away in the morning and it will be stored securely until the end of the day.

Staff must ensure their phones are off during teaching time. Staff (teaching and non-teaching) must not use mobile phones in the company of pupils. It is not permitted to use mobile phones on the school yard during playtime or outdoor class activities.

All visitors to the school including (but not exclusively) nurses; social workers; peripatetic teachers; tradespeople; Governors; students and volunteers must not have mobile phones turned on in the company of pupils. All visitors will be reminded to turn their mobile phone off when they sign in. In the event of an emergency where staff need to keep their mobile phone on in class, they should request permission from the Head teacher or Deputy Head teacher.

Under no circumstances must photographs or videos be taken of school children on personal devices. Cameras and mobile phones are prohibited in all toilet areas.

Use of digital media

Under GDPR, the school must seek parental consent to take photographs and record the children. Photographs can only be published with pupil/parent/carer consent. Printed copies will only be used for school displays and as evidence in pupils' workbooks. When displays are taken down, photographs will be returned to the child whose image was used and not shared with any other children. If a child does not want their photograph, it will be destroyed in confidential waste.

An image consent form will be sent out to all parents/carers annually. The form will include consent for the use of images as evidence of children's work, for displays, for the school website and for Class Dojo.

Photographs used for St Mary's Catholic Primary School website will always be anonymous. Photographs used in press releases will contain first names (if required) having previously obtained parental consent.

It is acknowledged that often photographs may contain other children in the background. Staff are asked to take care when taking photographs to ensure the privacy of each individual. Photographs containing pictures of those children who have requested not to be included or whose parents/carers have not consented must be destroyed.

We accept that parents may wish to photograph or record certain events during the school calendar. Parents who would rather their child was not photographed will be given the opportunity to discuss possible solutions with their child's class teacher. Parents who attend school events are all made aware before the event that images of other children should not be taken nor shared on social media.

ClassDojo

Each class within the school uses ClassDojo as a positive reward system. ClassDojo allows teachers to reward pupils with points for positive behaviour. In setting up their class account, teachers will only enter the children's first names. The ClassDojo privacy policy can be found online at https://www.classdojo.com/privacy/ and states, 'ClassDojo has been certified by iKeepSafe, an FTC-approved COPPA Safe Harbor, for compliance with their COPPA Safe Harbor program. Children are not required to provide personal information beyond that which is reasonably necessary to use ClassDojo. Information collected from students on ClassDojo is **never** used or disclosed for third party advertising or any kind of behaviourally-targeted advertising, and it is **never** sold or rented to anyone, including marketers or advertisers.'

Teachers may decide to utilise the Class Story on ClassDojo which enables them to post photographs and updates about activities and work completed within the school day. In order to post a photograph of a child, consent must be obtained from parents using the Image Consent Letter sent out at the start of each year. Teachers must not use names alongside any photographs. Parents/carers can also sign up to receive updates and notifications about their child's positive behaviour choices and are given individual usernames and passwords. They can also view the Class Story. Parents are not permitted to share any photographs from the Class Story on social media or by forwarding any images to other parents. This is made clear on the Image Consent Letter.

ClassDojo keeps teacher, school leader, and parent personal information until it is deleted, or until they are no longer needed to provide the ClassDojo service. They only keep student personal information for as long as the student's account is **active**, unless they are required by law to retain it, or need it to protect the safety of our users.

Links to the ClassDojo privacy policy can be found on the school website and parents will be made aware of the safe use of ClassDojo through letters and consent forms.

Communication Technologies

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at KS1, while pupils at KS2 can be provided with individual school email addresses for educational use if required.

- Pupils will be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Network sites

If a Social Network site is used personally by staff, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended. Staff must not communicate with children on any Social Network site. Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

The content posted online should not refer to school at all. This is to ensure that comments made by staff do not;

- bring the school into disrepute
- lead to valid parental complaints
- be deemed as derogatory towards the school and/or its employees
- be deemed as derogatory towards pupils and/or parents and carers or bring into question their appropriateness to work with children and young people

In incidents where parents post inappropriate comments about staff or children that could be construed as instances of cyberbullying or post images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own, staff must inform the Head teacher who will decide on the appropriate action to take.

Dealing with incidents

The school’s E-safety champion (Mrs O’Mahony) and the DSL team will be responsible for dealing with E-safety incidents. An incident log will be used to record and monitor offences and will be located in Mrs O’Mahony’s office. It will be monitored and reviewed on a regular basis.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). The head teacher must never personally investigate, interfere with or share evidence as this may inadvertently be an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix). Always report potentially illegal content to the Internet Watch Foundation (http://www.iwf.org.uk). **They are licensed to investigate – schools are not!**

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website http://www.iwf.org.uk

Inappropriate use

It is important that any incidents regarded as inappropriate use are dealt with quickly and actions are proportionate to the offence.

Incident	Procedure/Sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action in line with the school behaviour policy.
Using other people's logins and passwords maliciously.	• Inform SLT or designated E-safety Champion. • Enter the details in the Incident Log.

Deliberate searching for inappropriate materials.	• Additional awareness raising of E-safety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • The Head teacher will consider whether to contact parents.
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

Reviewed: March 2024
Review Date: September 2025