St Mary's R.C. Primary School
E-Safety Policy

Feb 2024

Vision:

We believe that every child is a gift from God, therefore, we aim to provide an outstanding and happy Catholic education which develops the 'whole child' whilst enabling them to reach their full potential.

Mission statement:

We love God … so we follow the examples of Jesus

We love learning … so we always do our very best in everything

We love each other … so we treat each other as we want to be treated

St Mary's R.C. Primary School E-Safety Policy

Vision:
We believe that every child is a gift from God, therefore, we aim to provide an outstanding and happy Catholic education which develops the 'whole child' whilst enabling them to reach their full potential.

Mission Statement:

We love God … so we follow the examples of Jesus

We love learning … so we always do our very best in everything

We love each other … so we treat each other as we want to be treated

Overview

The focus for this policy is to ensure that existing Policies (such as those on child protection and anti-bullying) are applied to the digital environment. In order for this to happen these Policies are regularly reviewed against the Local Authority's and national guidance, and updated as necessary.

Objectives
- To manage on-line technology so that children are kept as safe as possible
- To respond as necessary when a risk to a child is discovered

Safeguarding children, including e-safety is everyone's responsibility; e-safety is, therefore, not just the responsibility of the computing coordinator but is a whole school approach. It is planned for and taught discreetly, and within the computing curriculum, but also on an ad hoc basis when necessary.

The overall aims of this Policy are to ensure that children:

- are equipped to access risks in a digital environment
- are enabled to make informed judgments about such risk, how to respond to and protect themselves from potential risks
- know what to do if something 'not quite right' happens (e.g. they are exposed to inappropriate content or undesirable contact)

Strategies

Teaching and Learning
Whilst recognising the considerable benefits of new technologies, we teach children to protect themselves from:

- Inappropriate content
- Undesirable contact
- Hurtful conduct

These are referred to as the three C's (Content, Contact and Conduct) and underpin all aspects of our approach to e-safety. We also use the 5 SMART targets.

The 'Five **SMART** E-Safety Areas' are as follows:

S – Safe – This gives the children an overview of how to keep safe on the internet, from what information to share online to who you are speaking to. As well as this, the children are advised when and where to use personal devices, such as mobile phones and IPADS.

M – Meeting – This makes the children aware that meeting someone online is extremely dangerous and that it should not be done under any circumstances. 'Online Friends Stay Online!'

A – Accepting - This focuses on potential problems that can arise from opening unknown files, E-Mails, Texts, etc.

R – Reliable – This shows the children how easy it is to be misled either on the internet or over the phone, via text. As well as this the children are made aware of the fact that not all the information they find and read online is always true.

T – Tell – This highlights that it is vital to tell somebody, like a friend, Teacher, parent or a responsible child (eg Head Boy/Girl or responsible older children, Prefects, GIFT team members etc) if they have got any issues. We also cover Cyber-Bulling and its effects.

Research indicates that children who are given greater freedom at school to use new technologies have a better knowledge and understanding of how to stay safe online. It is, therefore, important that the school runs a 'managed system' that helps children to become safe and responsible users of technology by allowing them to take more responsibility and manage their own risk. We believe that children become more vulnerable if they are not given the opportunity to learn how to assess and deal with online risk for themselves.

Why We Use On-line Technology?
The purpose of using on-line technology in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance

the school's management information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

How Does On-line Technology Enhance Learning?
The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Children are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval.

Managing the Use of On-line Technology

Acceptable Use Policy (AUP)
This sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. The AUP details how we provide support and guidance to parents/carers for the safe and responsible use of these technologies by adults and children. Each user signs a contract to ensure that they know what is deemed 'acceptable use of the Internet'. All staff and children sign a form at the beginning of the Year and students and any new staff sign as part of their induction.

The E-safety Lead
At St. Mary's RC Primary School there are two E-Safety leads – Mr Jenkins (Computing Subject Leader) and Mrs Ruane who is also the designated person for Child Protection/DSL. The responsibilities of the leads include:

- updating the AUP
- ensuring that Policies and procedures include aspects of e-safety for example the Anti-Bullying Policy includes cyber-bullying
- working with EDIT (School's IT Company) to ensure that filtering is set atthe correct level for staff and children
- ensuring that staff training is provided on e-safety issues each year
- ensuring that e-safety is included in staff induction
- ensuring e-safety is covered by the children regularly
- monitoring and evaluating incidents that occur to inform future safeguarding developments

Monitoring and keeping updated as to new apps and potentially dangerous technology and sharing with staff and pupils

Password Security
Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. All users read and sign an Acceptable Use Contract to demonstrate that they have understood the school's E-safety Policy.

- Staff are provided with an individual email log-in username

- Staff are instructed to inform the e-safety lead if they think their password has been compromised or someone else has become aware of their password
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and MIS including ensuring that passwords are not shared and are changed periodically
- Staff should ensure that computers and lap tops are password protected and not left unattended
- All work, data and images stored on portable devises must be password protected or encrypted – Staff have been supplied with encrypted USB sticks. Egress is used to transfer sensitive data

All staff have been GDPR trained and are updated on changes and new requirements

Managing Specific On-line Technologies

Internet Access

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form giving permission for their child to use the Internet.

- In Foundation Stage and Key Stage 1, access to the Internet is by adult demonstration and direct supervised access to specific, approved on-line materials
- In Key Stage 2, pupils will work at times independently using the Internet, but will not be left unsupervised. We have very strong firewalls too. Pupils are taught the importance of e-safety and agree terms and conditions for acceptable Internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may be not always be reliable or accurate

The School Website:

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published
- Web site photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website

Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms
- Pupils will not access social networking sites for example 'Snapchat, 'Facebook', 'Twitter/X', 'Instagram 'etc
- Any form of bullying or harassment is strictly forbidden

Filtering

- The School works in partnership with parents, EDIT and DfE advice to ensure that systems are in place to protect pupils (DfE statutory guidance was updated Sep 2023 and further measures for filtering and monitoring are now in place, following additional staff training)
- If staff or children discover unsuitable sites, the URL (address) and content must be

reported to EDIT via the E-safety lead/DSL – we have additional support from EDIT now who do weekly checks on our internet usage across the school and run a detailed report. If any inappropriate or worrying content has been searched for, we then follow the below systems regarding how to respond if a risk is recovered

- Any material that the school believes to be illegal must be referred to the Internet Watch Foundation (IWF)

Photographic, video and audio technology

- It is not appropriate to use photographic or video devices in changing rooms or toilets
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed
- Staff may use photographic or video devices (including digital cameras and school iPads – not personal mobile phones) to support school trips and curriculum activities. School equipment should be used for this purpose. Personal equipment should not be used for taking school images, then all images must be transferred to school hardware and deleted from the personal device as a matter of urgency
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken
- Pupils should always seek the permission of their Teacher before making audio or video recordings within school grounds

Mobile Phones

- Children are not encouraged to bring mobile phones in school and are not allowed to use them in school. However, if older children (who may come to school on their own) bring a phone to school, they must hand it to their Teacher, switched off, who will store it safely for the day. We cannot accept any responsibility for loss or damage to any child's phone
- Staff must have their mobile phones away from view and on 'silent' during teaching times
- The sending of abusive or inappropriate text messages is strictly forbidden

Emerging ICT Applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed, and must ensure GDPR compliant

Radicalisation

- Procedures and Monitoring: It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach
- Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Designated Safeguarding Lead)
- Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils

Sexual Harassment

- Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting' or 'upskirting'; inappropriate sexual comments on social media; exploitation; coercion and threats).
- Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified. Our school follows and adheres to the national guidance in 'Keeping Children Safe in Education', Sep 2019

Complaints Regarding the Use of On-line Technology

Prompt action is required if a complaint is made. The facts of the case must be established and presented to the E-safety lead. A minor transgression of the rules may be dealt with by the Teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the School's Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Rochdale LA child protection procedures and our school Policy.

Any complaints about staff misuse of on-line technology must be referred directly to the Headteacher, who will take appropriate action.

How to Respond When a Risk is Discovered:

The E-safety lead will ensure that the following procedures are adhered to in the event of any misuse of the internet:

If an Inappropriate Website is Accessed Inadvertently:

- Report website to the E-safety lead
- Contact EDIT so that the site can be added to the banned or restricted list
- Change local control filters to restrict locally
- Log the incident

If an Inappropriate Website is Accessed Deliberately:

- Ensure that no one else can access the material by shutting down the computer
- Log the incident
- Report to the Head and E-safety lead immediately
- Head to refer back to the Acceptable Use Rules and follow agreed actions for discipline
- Inform the filtering services in order to reassess the filters

If an Inappropriate Website is Accessed Deliberately by a Child:

- Refer the child to the Acceptable use rules that were agreed
- Reinforce the knowledge that it is illegal to access certain images and police can be informed
- Log the incident
- Decide on appropriate sanction
- Notify the parent/carer

• Contact the filtering service (EDIT) to notify them of the website

If an Adult Receives Inappropriate Material:
• Do not forward this material to anyone else – doing so could be an illegal activity
• Alert the E-safety lead and Headteacher immediately
• Ensure the device is removed and log the nature of the material
• Contact relevant authorities for further advice e.g. police, social care CEOP
• Log the incident

<u>If an Illegal Website is Accessed or Illegal Material is Found on a Computer</u>:

The following incidents must be reported directly to the police:
• Indecent images of children found. (Images of children whether they are photographs or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
• Incidents of 'grooming' behaviour
• The sending of obscene materials to a child
• Criminally racist or anti-religious material
• Violent or bomb-making material
• Software piracy
• The promotion of illegal drug-taking
• Adult material that potentially breaches the Obscene Publications Act in the UK

If any of these are found, the following should occur:
• Alert the DSL/E-Safety lead immediately
• DO NOT LOG OFF the computer but disconnect from the electricity supply
• Contact the police and or CEOP and social care immediately
• If a member of staff or volunteer is involved, refer to the allegations against staff Policy and report to the Local Authority Designated Officer (LADO)

If an adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)
• Ensure the child is reassured and remove them from the situation
• Report to E-safety lead and designated person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection procedures
• Report to the Local Authority Designated Officer
• Preserve the information received by the child if possible
• Contact the police as necessary

If threatening or malicious comments are posted to the school website or facebook page (or printed out) about an adult in school:
• Preserve any evidence and log the incident
• Inform the Headteacher immediately who will then take any appropriate actions felt necessary
• Inform the E-Safety Leader so that new risks can be identified
• Contact the police or CEOP if appropriate

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to Headteacher or E-Safety lead.

If threatening or malicious comments are posted to the school website or facebook page about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

- Preserve any evidence and log the incident
- Inform the E safety Lead immediately and the Headteacher who will follow the Child Protection Policy
- Check the filter if an Internet based website issue
- Contact/parents and carers
- Refer to the Bullying Policy
- Contact the police or CEOP as necessary

Outcomes

That all staff are aware that safeguarding children, including e-safety, is everyone's responsibility; e-safety is, therefore, not just the responsibility of the computing coordinator, it is a whole school approach. Staff can manage on-line technology so that children are kept as safe as possible. As a school, we respond where necessary when a risk to a child is discovered. Children are equipped to access risks in a digital environment and are able to make informed judgments about such risk. Children know how to protect themselves from harm and know what to do if something 'not quite right' happens (e.g. they are exposed to inappropriate content or undesirable contact). Learning online is a positive experience for everyone in our school. We learn about and we learn from technology. Although we promote the enjoyment of online learning and use of technology across the curriculum, we are always proactive and vigilant to the potential dangers.

Date: **Sept 2014**

Signed: **Chair of Governors**

Reviewed: **Mar 2016**
Reviewed: **Jan 2018, Jan 2020**
Reviewed: **Feb 2022, Feb 2024**