Approved: FGB 28.11.23

St Monica's Catholic Primary School

Online Safety Policy

Publication Date: November 2023

Review Date: November 2024

St Monica's Catholic Primary School

Online Safety Policy

1. Philosophy

Every child is a unique gift from God, with his or her own unique gifts.

At St. Monica's, we strive to ensure that all children are offered the opportunity to develop to their full potential in individual, educational, moral, intellectual and spiritual needs.

Our school aims to be a living community of work and prayer.

We believe in supporting all staff, teaching and non-teaching, in meeting their individual needs and developing the staff as a team.

2. Introduction

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st Century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access.

At St Monica's we are dedicated to ensuring that our pupils have the skills and knowledge they need to evaluate internet information and to take care of their own safety and security when using the internet both inside and outside of school. This policy aims to establish procedures to identify, intervene and escalate any incident where appropriate.

Children at St Monica's are taught about how they can keep themselves and others safe, including online. To be effective, we present this information in an age-appropriate way. We are sensitive to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.

Keeping Children Safe in Education (DfE 2023) highlights that 'The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of

nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Information and Communication Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies pupils use inside and outside of the classroom include:

- Websites
- E-mail, Instant messaging and chat rooms
- Social media including, Facebook, Twitter, Snapchat and Instagram
- Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices with web access
- Gaming, particularly online gaming
- Learning platforms and Virtual learning environments
- Blogs
- Podcasting
- Video broadcasting
- Music downloading

The internet is a fantastic resource when used safely but often usage is not monitored consistently, therefore we aim to ensure that all pupils and staff are aware of the risks associated with these internet technologies.

At St Monica's we are dedicated to educating all pupils about online safety to ensure they have the skills they need to behave appropriately, think critically and keep themselves both safe and legal when using the internet and related technologies, in and beyond the context of school.

3. Role and Responsibilities

The Senior Leadership Team and the Governors of St Monica's have developed a policy which highlights practices and procedures which will be used to keep all children safe.

The Online Safety Leader will work with the Senior Leadership Team and the Governors to monitor systems and ensure that it is embedded into on-going School Development and is an important aspect of strategic leadership.

The policy will be reviewed annually and will be approved by the Governing Body.

This policy, supported by the school's Acceptable Use agreements for staff and pupils, is to protect the interests and safety of the whole school community. It is linked to the following policies:

- Child Protection
- Anti-Bullying Code
- Behaviour Policy
- Health and Safety
- Staff Code of Conduct

4. Online Safety in the Curriculum

The purpose of Internet use in school is to raise educational standards, to promote pupil's achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. It is increasingly used across the curriculum in order to prepare our pupils for the world around them. Therefore, at St Monica's we believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote it, such as celebrating 'Internet Safety Awareness day' in February.

By the end of primary school, pupils will know:

That people sometimes behave differently online, including by pretending to be someone they are not.
That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when they are anonymous
The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
How information and data is shared and used online
What sorts of boundaries ae appropriate in friendships with peers and others (including in a digital context)
How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Pupils with Additional Needs

Staff at St Monica's are aware that some pupils may require additional support or teaching to ensure they fully understand how to keep themselves and others safe online. Where a pupil has specific educational needs, resources are adapted, prompts and reminders are designed and

further teaching and explanations are provided to ensure they access the learning and their awareness is enhanced. Internet activities are differentiated and assessed accordingly.

6. Staff Training

All staff will have regular safeguarding training which includes online safety to ensure they are up to date with latest legislation and that online safety is kept as a high priority in all areas of their teaching. Teachers and Support staff will also take part in an annual E-Safety online course with Smartlog. The school fully complies with the PREVENT duty and is aware of the risks surrounding Child Sexual Exploitation. Through rigorous staff development and clear safeguarding procedures, the school is dedicated to keeping children safe online.

7. E-Mails

The use of E-Mails within school is an essential part of communication and should be treated with respect. In the context of school, e-mails should not be considered private. We understand that e-mail is an important aspect of online technology and we aim to equip our pupils with the skills they need to send and receive e-mails.

To ensure transparency and safety there are guidelines around the use of e-mails within school:

- All staff are provided with a school e-mail account to use for all school business. This is to protect staff and minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal details being exposed
- To ensure safety and security, all mail is filtered and logged; if necessary e-mail histories can be traced.
- The account holder is responsible for keeping the password secure and ensuring that the account is used for all school-based business.
- Staff should not contact pupils, parents or conduct any school business using personal e-mail addresses
- E-mails written from the school account should be treated in the same way that letters using school headed paper are. They should be written carefully, professionally and are proof-read.
- Pupils may only use school approved accounts for educational purposes and should be monitored at all times
- School e-mails will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Whole class or group e-mails should be used in school
- The forwarding of chain letters is not permitted in school.
- E-mails must not be used by any member of the school community to send or receive indecent or offensive images, videos or written material of this kind. In addition, emails

- E-mails should not be used to cause intentional harm or upset, directly or indirectly to others.
- Pupils must immediately tell an adult if they receive offensive emails before it is deleted
- All staff must inform the Online Safety Lead or Headteacher if they receive an offensive email whether it is directed at them or others, before it is deleted

8. The internet

There are numerous benefits to using the internet and it is available to everyone at all times. All use of the internet is filtered and monitored. Whenever inappropriate use in detected, it will be followed up accordingly.

To ensure safe use as St Monica's we ensure that:

- All staff sign an 'Acceptable Use' agreement (Appendix 1)
- A current record of all staff and pupils who have internet access in maintained
- Parents have signed and returned a consent form for pupil access
- Staff will research and check any internet sites prior to use with pupils
- Pupils have clear procedures for minimising and reporting if they discover an unsuitable site
- If an unsuitable site is discovered, all staff will note the URL, time and content and will report to the Online Safety Lead or ICT support services
- All users must observe copyrights for school software or online materials at all times
- On-line gambling or gaming is not allowed
- Up to date filtering and monitoring technology is used and understood by the DSL and Headteacher

9. Artificial Intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/ carers ,be familiar with generative chatbots such as ChatGPT and Google Bard.

At St. Monica's we recognise that AI has many uses to help pupils learn, but may also have potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

St. Monica's will treat any use of AI to bully pupils in line with our anti-bullying/ behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

10. Taking images and/or films and storage

Digital images are easy to capture and can be a wonderful tool for documenting learning and life experiences. It is important to remember that in order to take, use and store images, consent first needs to be sought. With the written consent of parents (on the behalf) of pupils, St Monica's permits the appropriate taking of images by staff and pupils with school equipment.

- Staff and visitors are NOT permitted to use personal equipment such as phones, cameras or tablets to record images of pupils. Only school equipment can be used. The images should then be saved onto the secure network and deleted from the individual device.
- Staff must check the children's consent forms before any image can be uploaded for publication
- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that arrangements are in place to ensure images are not stored or distributed outside of the school

Images and films are stored securely on the school's network and right of access to this material is restricted to teaching staff and individuals within the confines of the school network or other online school resource.

11. Published content and the School Website

The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupil's personal details will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

12. Publishing pupil's images and work

Permission from parents and the pupil will be sought prior to any publication and children's full names will not be used anywhere on the school website. Pupils' images and work will not be used for social media unless it is on a school approved site which is monitored and used appropriately.

13. Video Conferencing

Permission is sought from parents and carers if their child is involved in video conferencing and it is always supervised by an adult. Approval is always sought from the Headteacher prior to video conferencing and clear records of date, time and participants are kept.

14. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should not use mobile phones or personal recording equipment to take pictures or videos of children.
- Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and all visitors. Mobile phones may be used in office areas, the staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/ visit outside of school, for use in emergencies only.
- Pupils who bring mobile phones to school are required to hand them in to school office staff every morning and collect them at home time.
- Staff/ visitors bringing personal devices into school must ensure there is not illegal or inappropriate content on the device.

15. Social Networking for pupils

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social networking space
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.
- Where incidents or concerns regarding children's use of social media outside of school are identified, the school will inform the parents or responsible persons immediately.

16. Social Networking for Staff/ Visitors

When using personal social networking sites such as Facebook, Twitter, Instagram etc..., staff should ensure that they:

- Do not make reference to their place of employment.

- If you do refer to your place of employment then a disclaimer is used, such as 'the views contained in these web pages are my personal views and do not represent the views of the school.'
- Do not use the school logo on any personal web pages
- Be aware of using material from copyrighted sources without permission
- Carefully avoid bringing the school or its employees into disrepute and consult your Headteacher if you are unsure whether the content is appropriate
- Understand that the school has the right to remove any content which may adversely affect the school's reputation or create risk of legal proceedings against the school.
- Do not reveal information which is confidential to the school.
- Employees must not use social networking sites for party political purposes
- Do not include or use any school data, information, contact details or photographs of employees, pupils, parents or partner organisations without the explicit written permission of the school and the data subject.
- Do not include comments which could bring into question your professional credibility.
- Time spent accessing social networking sites at work, for personal use, using school equipment must comply with this policy and includes the use of school equipment at home or outside of working hours.
- Do not invite or accept as 'friends' on such sites, any child or the family members of any child you have met in the course of your employment.
- If you receive press or media contact regarding the content of your personal site and feel there may be implications for you or which in any way relates to the school, you should consult the Headteacher.

17. Information System Security

St Monica's school ICT systems capacity and security will be reviewed regularly and virus protection will be installed and updated regularly. St Monica's will work in line with Local Authority procedures.

18. Protection Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must 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.

We will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only 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.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media:
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

19. Assessing the Risks

The school will take all reasonable precautions, using our filtering and monitoring, to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

St Monica' will filter and monitor the use of ICT to establish if the online safety policy is adequate and that the implementation of the policy is appropriate.

20. Handling Online Safety complaint

- Complaints about internet misuse will be dealt with by a member of the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature should be dealt with in accordance to the school's child protection procedures

- Pupils and parents will have access to the complaints procedure
- Any potential illegal issues will be dealt with accordingly, taking advice from the police where appropriate and any concerns relating to the PREVENT duty will be reported to CHANNEL in-line with government guidance.

21. List of Appendices

Appendix A- Acceptable Use Agreement

Appendix B- Laptop Agreement

Appendix C- Parental Agreement

This policy will be reviewed annually.

Appendix A

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary

that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix B

St. Monica's Catholic Primary School

Employee Laptop Agreement

I accept the following responsibilities:

1. I understand that the laptop computer is the property of St. Monica's School and is issued to employees for the purpose of conducting school business. It is intended only for the use of the school employee to whom it is assigned and shall not be loaned to any persons without permission.
2. The laptop computer is a desktop replacement, therefore it must be at school during regularly scheduled work days in order to receive administrative communications, upgrades to anti-virus and other software, to take daily attendance and other requirements of the student records management system, etc.
3. The laptop computer may be taken home or to other locations after school hours by the employee. However, the employee is responsible, at all times, for the care and appropriate use of the laptop computer.
4. I will not disable or uninstall the virus protection program that is provided with the machine.
5. I will use the computer for school or professional development purposes. I will not install any
   software on the computer unless it has been approved by the school's IT Support at St. Pauls.
6. I will ensure any documents I create will be moved from the laptop to the network on a monthly basis for backup purposes.
7. I will report any problems/issues I encounter while using the laptop to the technology department immediately. **Email: icthelpdesk@st-pauls.org.uk Urgent Support Tel: 01908 359799**
8. I will not write on or place any labels or stickers on the laptop.
9. The laptop is issued to you in your current teaching position. If you change positions the laptop may be reassigned to other teachers.
10. The laptop computer will need to be returned to IT Support from time to time to receive regular maintenance and upgrades. You will be notified when this becomes necessary.
11. School policies regarding appropriate use, data collection, computer misuse must be adhered at all times.
12. All laptops must be returned at the end of the school year for inventory and software updates.
    Laptops will be reassigned as deemed appropriate.

Full Name(Print)……

……..

Job Title

……..

Employee Signature……. Date…….
Laptop Make/Model…….Serial Number…….

Appendix C

Internet Use

The school has installed computers and internet access to help us learn. These rules will keep everyone safe and help us to be fair to others.

- I will not open other people's files
- I will not bring disks in from outside school
- I will not try to delete anything from the computer except my own work
- I will only use the internet if I have permission from a member of staff
- I will only send e-mails to people I know and with my teacher's permission
- I will use materials such as paper and ink responsibly
- I will not give out my home address or telephone number or arrange to meet anyone
- I will report any unpleasant material I find on the internet and I will not deliberately try to access unpleasant material
- I understand that the school will check my computer files and may monitor my computer and Internet usage

Children's agreement

I understand the school rules about using computers sensibly in school.

Child's Name:……..

(BLOCK CAPITALS)

Signature of child: _____ Date: _____