St Mary's C.E. Primary School

E-Safety Policy

Revised October 2025

Policy for E-Safety

"With God, all things are possible" Matthew

Rationale

The purpose of Internet use 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 administration systems.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Internet use is an essential element in 21st century life for education, business and social interaction. Therefore, access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

How can internet use enhance learning?

- The school internet access is designed for pupil use and includes filtering by Stockport Local Authority, appropriate to the age of the pupils
- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games

- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Authorised internet access

- The school will maintain a current, electronic record of all staff and pupils who are granted internet access
- Parents and children themselves must read and sign the relevant section of the Acceptable Use Policy at the beginning of each academic year (Appendix A)
- All staff must read and sign the Staff Acceptable Use Policy at the beginning of each academic year.(Appendix B)

Evaluation of internet content

- If staff or pupils discover unsuitable sites, the URL (website address), must be reported to the Headteacher and Computing subject leader for appropriate action, then reported to Stockport LA, who will block the website from school's devices
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law
- Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Email

- Pupils may only use their email accounts on Purple Mash during a school day. Only children and staff in our school can be contacted by Purple Mash email and there is no way to allow for contact of anyone outside of school. These email accounts are monitored by teachers and are only used during lesson times.

- Pupils must immediately inform a member of staff if they receive an offensive email in school.

- Pupils will be taught how to safely send and receive appropriate emails as part of the Computing curriculum. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet with anyone. Fake email simulations are set up for the purpose of online safety.

- Access in school to external personal email accounts may be blocked if a child is found to be accessing this in school.

Social networking

- The school will not allow pupil access to social networking sites unless a specific use is approved (e.g. forums on a school blog).

- Pupils are advised never to give out personal details of any kind which may identify them or their location.

- Pupils are advised not to place personal photos on any social network space and parents are advised to place all privacy settings on high.

Filtering

The school will work in partnership with Stockport Local Authority to ensure filtering systems are robust and as effective as possible. If staff or pupils discover unsuitable sites, the URL (website address) and content must be reported to the Headteacher and the Computing subject leader who will report this to the LA.

USB memory sticks and other portable data storage devices

- Staff to consider what data should be stored on USB sticks / other data storage devices

- Sensitive data should be encrypted

Storage of photographs

- Photographs are to be stored in once place, in a secure area with the school network.

- Photographs are to remain on school premises. Where photographs have been taken for school trips, the images are downloaded to the school network as soon as possible.

- Photographs are to be deleted off devices once they are downloaded onto the school network.

- The current LA policy is adhered to regarding photographing and publishing images of children.

- Publishing of photographs on our school website / X page will only be done with parental permission, which parents give when their child starts at St. Mary's. Pupil's full names will not be used anywhere on our school website or X page in association with any photographs.

Mobile phones and other handheld devices

- Mobile phones and other handheld communication devices are not to be used for personal use in formal school time by staff or pupils.

- For the purpose of security, we recognise that parents / carers of KS2 children may want their child to bring a mobile phone to school. If this is required, all phones will be turned off and handed into the school office in the morning for safe-keeping, They will be handed back out to children at the end of the day.

- Children are only allowed to turn on their mobile phone when outside of the school grounds.

- Sending of abusive or inappropriate messages is forbidden.

- Outside of school hours, children are discouraged from taking photographs and videos on school grounds and is classed as an infringement of personal privacy.

Published content and the school website

- The contact details on the website will be the school address, email and telephone number. Personal information of staff or pupils will not be published.

- SLT will take overall editorial responsibility and ensure that content is accurate and appropriate.

Information System security

- School ICT systems and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Assessing Risks

St. Mary's CE Primary School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. That said, the school recognises that by adapting a managed IT system, pupils will develop a better knowledge of how to stay safe online as they develop the ability to assess and manage risks for themselves. Neither the school nor Stockport Council can accept liability for the material accessed, or any consequences of internet access. The school will audit the E-safety guidance every twelve months, to establish if it is adequate and that the implementation of the guidance is appropriate.

Handling E-safety complaints

- Any complaints of internet misuse will be dealt with by a senior member of staff, safeguarding lead or headteacher.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the child protection policy.
- Pupils and parents will be informed of the complaints procedure.

Staff and the E-Safety policy

- As part of the ongoing commitment to staff professional development, the school conducts an audit of training needs of all staff and provides training where required to further their knowledge, skills and expertise.
- All staff has access to the school E-Safety policy to ensure they are aware of current and up-to-date guidance.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- St. Mary's Child / Parent E-safety Agreement (Appendix A)

Pupils' use of ICT Equipment and the Internet

The school uses filtered Internet service, which minimises access to undesirable material. Pupil access to the school network and internet will be controlled by the following measures:

- staff members will explain to pupils the school's expectations of appropriate conduct;
- staff will explain to pupils what to do if they came across inappropriate material;
- while pupils' use of the Internet will generally be supervised, it is neither possible nor desirable to guarantee that **all** use will be observed by staff;
- pupils' e-mail and other Internet-related files and history will be monitored by staff to ensure that expectations of online behaviour are being met;
- pupils must ask permission to use the Internet and have a clear idea why they are doing it;
- pupils are not allowed to contact people who have not been approved by their teacher;
- pupils are not allowed to use rude language;
- pupils may not login using other people's names or passwords;
- pupils must not access other people's files;
- pupils may not copy files onto the school network;
- pupils may bring work from home on a CD or USB device; however, this must be submitted for secure virus checks **before opening** any files onto school's system / network;
- pupils must not give out personal information such as phone numbers.

Sanctions for non-compliance

Pupils who choose not to comply with these rules will be subject to general discipline procedures. Persistent misuse of the Internet by pupils will result in a fixed period when access is banned. In such cases parents will always be notified. Misuse of other technologies may lead to bans, confiscation or other sanction.

Pupil Agreement

Child's Name _____

I have read and understand the above.
I will use the internet access, iPads and laptops in a responsible way at all times.
I know that my behaviour and activity will be monitored.
I understand that if I break the e-safety agreement my equipment may be confiscated and my access to the network may be suspended. If this happens, my parents will be informed.

Parent/Carer Agreement

I have read and understand the above and I give permission for my child to access the internet. I understand that St. Mary's CE Primary School will take all reasonable precautions to ensure that my child is a safe and responsible digital user.

Signed _____

St. Mary's Staff ICT Code of Conduct (Appendix 2)

♣ I will ensure that I keep my password safe.
♣ I will ensure that I securely log off from any workstation I use during the day.
♣ I will safeguard the speed of the network by selecting the most appropriate time to download large resources or watch on-line TV content.
♣ I will clean up unused files from the network to assist with the longevity of disk storage devices.
♣ I will ensure I remove any portable storage devices or media that I use in the school computers
♣ I will password protect any confidential or sensitive information that I store on portable storage devices.
♣ I will not open any attachments, executables or files from unknown or untrusted sources.
♣ I realise that school ICT space is not personal space.
♣ I will not take copies of any materials that belong to or are the intellectual property of the school.
♣ I will leave copies of any planning or resources, created using ICT, that are required by the school.
♣ I will not use the school ICT equipment for personal financial gain, gambling, political activity, advertising or illegal purposes.
♣ I will not to reveal personal information about the pupils I teach or the school through email, personal publishing, blogs or messaging.
♣ I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
♣ I will not install any software or hardware without permission.
♣ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
♣ I will report any incidents of concern regarding children's safety to the e-Safety Coordinators, and the Designated Safeguarding Lead.
♣ I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read and understand the rules of ICT use.

Name: _____