St Mark's RC Primary School e-safety Policy

This policy applies to all members of the school community (including staff, students, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of St Mark's RC Primary School's computing systems.

What is e-safety

E-safety means electronic safety. It is concerned with the protecting of young people in the digital world and ensuring they feel safe when accessing new technology.

The Internet is a fantastic resource for learning and is becoming easier and easier to access with the advances in mobile devices like smartphones, iPads and tablets, as well as the more traditional PCs and laptops. It is very important that our whole school community – pupils, staff, governors and parents/carers/families - are aware of the potential risks, as well as the obvious benefits of using the Internet and this policy aims to help to create and maintain a safe digital environment for St Mark's.

1. E-safety Policy

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's e-safety coordinator is Mrs Miller
- The e-Safety Governor is Mrs Patterson
- The e-safety Policy and its implementation shall be reviewed annually.
- It was approved by the Governors on: 9th February 2017

Roles and Responsibilities

E-safety should be included in all areas of the curriculum and staff should reinforce e-safety messages regularly in lessons. The e-safety curriculum should be broad and balanced and provide progression with opportunities for creative activities and will be provided by:

- A planned e-safety curriculum delivered as part of computing lessons
- Staff acting as good role models in their use of digital technologies, the Internet and mobile devices.
- Key e-safety messages reinforced in assemblies and cross curricula lesson time
- Clear guidance in lessons where Internet use is planned; it is best practice that pupils should be guided to sites checked as suitable for this and that processes are in place for dealing with any unsuitable material that might be found

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the e-Safety Co-ordinator.(annually)
- Regular monitoring of e-safety incident logs (CPOMS). (termly)
- Reporting to relevant Governors committee / meeting.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD opportunities to enable them to carry out their e-safety roles and to train other colleagues, where relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher working with the E-safety co-ordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

The e-safety co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy / documents.
- Working with the Headteacher, ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Undertakes training and provides training and advice for staff
- Liaises with the Local Authority, IT Assist and Gem Education
- Liaises with school technical support staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the e-Safety Governor to discuss current issues and review incident logs.
- Attends relevant meetings.

2. Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff, parents/carers and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

St Mark's RC Primary School e-safety Policy

- The school Internet access will be directed for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new Computing Curriculum, all year groups will experience e-safety lessons and be regularly reminded about staying safe on line. These lessons will include topics from how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through Computing we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEN co-ordinator and individual teachers to ensure all children have equal access to success in this subject.

3. Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable Use' Policy before using any school computing resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

4. World Wide Web

St Mark's RC Primary School e-safety Policy

The Internet opens up new opportunities and is an essential part of the everyday world for children. Learning, homework and sharing through social media are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident on CPOMS. This will be reviewed termly by the e-Safety Co-ordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Pupils will be taught to be responsible when using the World Wide Web.
- The school will work in partnership with ITAssist to ensure filtering systems are as effective as possible.

5. E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Pupil access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

6. Social Networking

Social networking Internet sites (such as Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors may consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.
- Pupils and parents/carers will be given information about using privacy settings
- Pupils and parents/carers will be shown how to report misuse/abuse on social networking sites

7. Cyberbullying

Cyberbullying will not be tolerated in our school- any kind of bullying is unacceptable (see our Anti-Bullying Policy).

- Any incidents of cyberbullying will be recorded on CPOMS and the incident dealt with in line with our Anti-Bullying Policy.

8. Mobile Phones/Devices

Many mobile phones/devices have access to the Internet and picture and video messaging and these can present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office as children enter school and can be collected at the end of the day, however school will not accept any responsibility for lost or damaged phones
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use a school phone to contact parents.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom during lesson time (unless it is being used as a teaching resource). All staff and visitors should ensure that their phones are turned off/in silent mode and stored safely away during the teaching day.

- Staff may use their mobile phones in the staffroom or classroom during the break/ lunch period, however phones should not be accessed in corridors and when children are in the vicinity.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- Pupils will be made aware that they are not allowed to take photographs/videos on their mobile devices anywhere on our school premises/grounds without permission.

9. Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff, with the understanding that images are strictly for personal use and not for publication in any manner.

10. 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 in consultation with ITAssist.

11. Published Content and the School Website

The school website is a valuable source of information for governors, parents/carers and potential parents/carers.

- Contact details on the Website will be the school address, e-mail and telephone number, as well as a contact person, e.g the Headteacher and Admin Officer.
- Staff and pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

St Mark's RC Primary School e-safety Policy

12. System Security

- School Computing systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with ITAssist
- E-safety will be discussed with our Computing consultant (GEM Education) and those arrangements incorporated in to our agreement with them.

13. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

14. Assessing Risks

The school will take all reasonable precautions 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 does not accept liability for the material accessed, or any consequences of Internet access. The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

16. Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions may be held with the community police officer to establish procedures for handling potentially illegal issues.

St Mark's RC Primary School e-safety Policy

17. Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- All pupils will be informed of the importance of being safe on social networking sites such as Facebook (objectives appropriate to age). This will be strongly reinforced across all year groups during Computing lessons and all year groups will look at different areas of e-safety during cross curricula lesson delivery.

Staff:

All staff will be given the School e-safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential (in line with Teacher Standards).

Parents:

Many parents/carers may have only limited understanding of e-safety and the risks/issues and may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet – they may also be unaware of how to respond. The school will therefore seek to provide information and awareness through this policy by:

- Drawing attention to the School e-safety Policy in newsletters, on the school Website and APP. Parents will receive regular invitations to attend e-safety chat/meeting and be invited to join children in e-safety lessons.
- Sending information regarding keeping children safe and their hardware protected to all parents/carers
- Issuing parents with a list of helpful websites if they wish to access further information on e-safety.

Written: January 2017

Next Review: January 2019