**St Martin’s C of E Primary School**

***‘Inspiring children to be the best they can be’***

**Online Safety Policy**

**Updated – Summer 2024**

**To be reviewed - Summer 2026**

**St Martin’s C of E Primary School**

**Online Safety Policy**

**1. Introduction**

Information Technology (IT) is an essential element in 21st century life for education, business and social interaction. The opportunities provided by the Internet are tremendous, both within school and outside. However, the Internet has brought with it new ways to hurt and abuse, including through cyberbullying, online grooming and sexual abuse of children. Therefore, schools have a safeguarding responsibility and a duty of care to provide students with good quality and safe Internet access as part of their learning experience.

This Online Safety Policy encompasses not only the Internet but also wireless electronic communications including mobile phones, games consoles and cameras. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using IT.

The aim is to provide safeguards and raise awareness, which will enable users to control their online experiences and feel confident and happy using technology.

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Furthermore, it is based upon the Surrey County Council Model Online Safety Policy and Toolkit for schools and updated with the NSPCC’s model online safety policy February 2022.

**2. Teaching and learning**

From September 2020, Relationships Education will be compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England. Through these new subjects, pupils will be taught about online safety and harms.

This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils’ lives. This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

**2.1. Why the Internet and digital communications are important**

* Internet use is a part of the statutory curriculum for Computing and a necessary tool for staff and pupils.
* Some of the many benefits of using the internet include:
  + Access to a wide variety of educational resources, including art galleries, historical sources, maps and information.
  + Rapid world-wide communication.
  + An increased understanding of people and cultures around the world.
  + Increased skills across the curriculum and in improving research and communication and collaboration skills.
  + Staff professional development.

**2.2. Internet provision at St. Martin’s**

* The school’s Internet access is provided through a British Telecom contract and educational web-filtering appropriate to the age of the pupils is provided by Securely Web Filtering and Parental Control.
* Pupils will be taught about which aspects of Internet use are acceptable and what is not and be given clear objectives for Internet use.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
* Pupils will be shown how to publish and present information appropriately to a wider audience.

**2.3. Children with Special Educational Needs**

* The school recognises that certain aspects of Online Safety are particularly challenging for certain pupils with special educational needs. For example, the most IT capable may also be the most vulnerable. Additionally, children who have poor social skills may be more at risk from inappropriate online contact.

**3. Managing Online Safety**

**3.1. System security**

* School IT systems’ security will be reviewed regularly.
* Virus protection will be updated regularly.
* Security strategies will be discussed with the Local Authority and agreed with the Governing Body.

**3.2. Accessing the internet**

* The internet is regularly used by teachers as a planned part of many lessons.
* All staff will review and evaluate resources on websites appropriate to the age range and ability of the pupils being taught.
* Access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
* As they gain experience, pupils become more independent, using searching techniques to locate information for themselves. An adult will always be present to supervise pupils; however, the teacher’s attention cannot be on every screen at all times.
* Pupils are taught to be critically aware of the materials they read, and that they might need to validate information before accepting its accuracy.
* Pupils will be taught how to report unpleasant Internet content either using the school’s 3Ts (Turn it over, Turn it off, Tell), or by using the CEOP link (<https://www.ceop.police.uk/safety-centre/>) via the school’s website.
* The school is aware that some Internet derived materials may have restricted access due to copyright law, and staff must comply with such law and ensure that pupils are aware of the laws also.

**3.3. E-mail - due to the way in which the children’s email accounts have been set, only mail from within the school’s domain will be received by children. They cannot send or receive mail from an external source nor can they send attachments when outside the domain.**

Pupils will be taught:

* To exchange information via an internal email address, to use an address book, to attach files to an email.
* To follow conventions of politeness.
* To tell a teacher if they receive an offensive email from another pupil.
* To not reveal personal details of themselves or others in e-mail communication, without specific permission.
* To not arrange to meet anyone they have met online, without specific permission.
* To treat all incoming e-mail with some suspicion, not opening attachments unless the author is known.
* How to present e-mail correspondence to external bodies.
* That forwarding of chain letters is not permitted.

Email communication between staff and pupils must only take place via a school email address. For example, staff members may not accept children onto their Facebook accounts.

*“Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.”* (Guidance for Safer Working Practice for Adults Who Work with Children and Young People, DCSF, 2007)

**3.4. Publishing pupil’s images and work**

* Parental permission is gained before images/photos of children are published on the school website, Pobble, or on social media platforms such as Twitter.

See: **USING IMAGES OF CHILDREN: PHOTOGRAPHS, VIDEOS, WEBSITES & WEBCAMS**

**3.5. The school website**

* The contact details on the website will be the school address, email and telephone number. Staff or pupils’ personal information will not be published.
* The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
* Photographs that include pupils will be selected carefully, taking account of the written parental/carer’s consent.
* Pupils’ full names will be avoided on the website.

**3.6. Google Classroom**

* The school has adopted Google Classroom as a learning portal. It is password protected, with different levels of security being available to different users.
* Children will be taught about the safe use of the school learning portal, before they are allowed to use it.
* The school’s Online Safety rules will be shared regularly with children and there is a link to the CEOP ‘Thinkuknow’ website from the school’s main site, explaining how children can report incidents should they feel concerned or uncomfortable online.
* Online forums within the learning platform are a means of facilitating discussion of Online Safety.
* Photographs that include pupils will be selected carefully, taking account of the written parental/carer’s consent.
* As the learning portal usage advances, the Computing subject leader will examine and risk assess new technologies before they are used.

**3.7. Social networking**

* There will be no access to social networking sites at school.
* Pupils and parents will be taught about the dangers that the use of social network sites outside school brings.
* Pupils will be advised to use nicknames and avatars when using social networking sites when they are at an appropriate age.
* Pupils will be taught never to give out personal details of any kind which may identify them or their location, or post personal photos.

**3.8. Managing filtering**

* The school will work in partnership with TAMAT to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher who will liaise with the DSL/Computing subject leader.
* The Designated safeguarding leads (DSL) are responsible for understanding the filtering and monitoring systems the school has in place. The DSL will monitor that the filtering methods selected are appropriate, effective and reasonable.

**3.9. Other technologies**

* Staff will use a school phone for all normal contact with parents’/carers’ homes. Personal mobile phones will not be used during lessons or formal school time. Personal mobile phones may be required on trips outside the school to contact the school office, or under unusual circumstances to call parents’/carers’ homes directly. The sending of abusive or inappropriate text messages is forbidden.
* The school is aware that as children become more independent in Upper Key Stage 2, they may walk to school, and bring mobile phones onto the school site. All children’s mobile phones will be turned off and locked away in a classroom locker during the day however, they remain the responsibility of the owner.
* Personal cameras, or cameras on mobile phones, will not be used for school business. School cameras will always be used.
* Images of children must not be downloaded onto personal computers; they must be downloaded to the school system and then deleted when appropriate. Games machines (including Playstations, Xbox and others) may be used for school use providing they do not have Internet access.
* Emerging technologies will be examined for educational benefit and assessed for risk, before use in school is allowed.

**3.10. Use of school equipment for home use**

* Generally speaking, school equipment must be used only for school business.
* Adults must have absolute control where a laptop is taken home. It must only be used by the staff member to whom it is allocated, and passwords should not be shared with anyone else.
* Staff members need to be aware that access to the wider internet at home increases the possibility of virus attack and potential identity theft.
* School laptops may not be used for illegal or inappropriate material. Illegal material includes possessing or distributing indecent images under 18; illegally downloading music etc. Inappropriate material includes: accessing adult pornography; ‘put downs’ on the basis of race, religion or orientation etc.; harassing or threatening individuals; making derogatory, offensive or insulting comments about pupils or colleagues.
* Staff need to be aware of the risks involved in storing and transporting confidential information. The safest storage location is the school network and or on the Cloud.

### 3.11. Protecting personal data

* Personal data will be recorded, processed, transferred and made available according to the revised Data Protection arrangement for the UK (GDPR) May 2018

**4. Policy Decisions**

**4.1. Authorising access to the school system**

* All staff and governors must read and sign the Acceptable Use Agreement (Staff Code of Conduct for IT) before using any school IT resource.
* The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
* Parents/carers will be asked to read the Online Safety rules and sign and return a Parental Consent form.
* Pupils will have been informed of the school’s IT rules and Online Safety guidance and will have signed a school IT agreement.
* Any person not directly employed by the school will be allowed access to the school network at the discretion of the IT subject leader.

**4.2. 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. Neither the school nor TAMAT can accept liability for the material accessed, or any consequences of Internet access.
* Cyber-attacks are one of the biggest threats that schools face. The school’s technical systems will be managed in ways that ensure that the school meets recommended technical requirements to mitigate such attacks. There will be regular reviews and audits of the safety and security of the school’s technical systems. Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to the school’s technical systems and devices.
* The Computing subject leader will audit IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

**4.3. Responding to an Online Safety incident**

* Complaints about Internet misuse by pupils will be dealt with by a member of the senior leadership team and will follow normal Behaviour Management policy/sanctions.
* Pupils and parents will be kept informed about any complaints procedure and the consequences for pupils misusing the Internet.
* Any complaint about staff misuse must be referred to the Headteacher.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
* Where relevant and if the circumstances allow, consideration will be given to informing the ISP (e.g. BT) or web host in order that appropriate action may be taken on their part to address the matter which might include, for example, their removal or blocking of offending material that has been accessed.

**4.4. Community use of the Internet**

* All use of the school Internet connection by community and other organisations shall be in accordance with the school’s Online Safety Policy.

**5. Communications**

**5.1. Sharing the Online Safety Policy with pupils**

* Appropriate elements of the Online Safety Policy will be shared with pupils.
* Online Safety rules will be posted in all networked rooms.
* Pupils will be informed that network and Internet use will be monitored.
* Curriculum opportunities to gain awareness of Online Safety issues and how best to deal with them will be provided for pupils.
* The school will recognise the annual Safer Internet Day and children will be involved in activities surrounding e-safety.

**5.2. Sharing the Online Safety Policy with staff**

* All staff will have access to the School Online 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 are essential.**
* Staff that manage filtering systems or monitor ICT use will be supervised by the senior leadership team and have clear procedures for reporting issues.
* All staff should continue to be provided with online safety information and training at induction, and receive online safety training as part of regular (at least annual) child protection training.

**5.4. Sharing the Online Safety Policy with parents. Enlisting parents’ support**

* Parents’ and carers’ attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
* Parents and carers will from time to time be provided with additional information on Online Safety.
* The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

**6. Statutory Context of Online Safety**

This section includes some of the statutory context surrounding Online Safety.

* Online Safety falls within the ‘Staying Safe’ strand of the ‘Every Child Matters’ agenda and KCSIE 2021 (updated 2022 and 2023).
* The Education and Inspections Act 2006, provides statutory powers for staff: to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises; to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with Online Safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.
* Ofsted judge the performance of a school in Online Safety.

**7. Key personnel**

The Computing subject leader acts as the Online Safety Coordinator.

The Designated Child Protection Lead Officers are: The Headteacher, the Deputy Head and the Special Needs Co-ordinator.

**8. Appendices**

Appendix 1: Online Safety rules (3Ts)

Appendix 2: Online Safety Guidance (i-smart)

Appendix 3: Parent/Pupil agreement (New starter packs)

Appendix 4: Staff, governor and visitor Acceptable Use Agreement (IT Code of Conduct)

Appendix 5: Pupil Acceptable Use Agreement

This policy was written and formally adopted by the School Governing Board at the meeting of the Wellbeing Committee - 05.06.2024.

Signed\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Review date – \_\_\_\_\_\_\_\_