St Martin's C of E Primary School

Online Safety Policy

Review date: Summer 2022

The purpose of our Online Safety Policy

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers; they may also arise through the use of other handheld devices such as games consoles and mobile phones.

Children interact with new technologies on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally, if not used correctly, place children and young people in danger.

Our Online Safety Policy covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes educating children on the risks and responsibilities of using such technologies safely and is part of the "duty of care" which applies to everyone working with children. St Martin's CE Primary School will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information in and out of the school environment. Current and emerging technologies used in school and more importantly in many cases, used outside of school by children include:

- The Internet.
- E-mail.
- Instant messaging often using simple web cams.
- Learning platforms.
- Blogs (as on-line interactive diaries).
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player).
- Social networking.
- Video broadcasting sites such as Youtube.
- Chat rooms.
- Gaming sites.
- Music download sites.
- Mobile phone with camera and video functionality.
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mails, web functionality and cut down 'Office' applications.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at our school:

- An effective range of technological tools.
- Policies and procedures, with clear roles and responsibilities.
- A comprehensive Online education programme for pupils, with staff and parents kept fully informed about internet E-Safety.

Who will write and review the policy?
The DSL/Computing manager, in partnership with the Head teacher, will write and ensure the implementation of the school Online Safety policy. The Online Safety Policy and its implementation will be reviewed annually. Our Online Safety Policy has been written by the school, building on the local and government guidance. It has been agreed by the Senior Leadership Team and approved by governors.

The DSL are:
Miss Sarah Bott
Mrs Kelly Lees
Ms Sharron Buff

Teaching and learning

Why is Internet use important?
Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside of school and need to learn how to evaluate Internet information and to take care of their own safety and security. 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 functions. Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?
Benefits of using the Internet in education include:
• Access to worldwide educational resources including museums and art galleries.
• Inclusion in the National Education Network which connects all UK schools.
• Educational and cultural exchanges between pupils worldwide.
• Vocational, social and leisure use in libraries, clubs and at home.
• Access to experts in many fields for pupils and staff.
• Professional development for staff through access to national developments, educational materials and effective curriculum practice.
• Collaboration across networks of schools, support services and professional associations.
• Improved access to technical support including remote management of networks and automatic system updates.
• Exchange of curriculum and administration data with LA and DFE.
• Access to learning wherever and whenever convenient.

How can Internet use enhance learning?
The school's Internet access will be designed to enhance and extend education.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
• Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
• Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?
Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
The evaluation of online materials is a part of teaching/learning in every subject. Online materials will be age appropriate and this will be reflecting in the level of evaluation that the children will be expected to undertake.
Children will undertake training on internet safety, including learning to evaluate sources of information and relating this to using the internet to enhance their learning.

Managing Information Systems
How will information systems security be maintained?
The security of the school information systems and users will be reviewed regularly.
Virus protection will be updated regularly.
Local Area Network security issues include:
• Users must take responsibility for network use.
• Workstations should be secure from casual mistakes by the user.
• Servers must be located securely and physical access restricted.
• The server operating system must be secure and kept up to date.
• Virus protection for the whole network must be installed and current.
• Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security issues include.
• Personal data sent over the Internet or taken off site will be encrypted.
• Portable media may not be used without specific permission followed by a virus check.
• Unapproved software will not be allowed in pupils' work areas or attached to email.
• Files held on the school's network will be regularly checked.
• The School ICT Technician will review system capacity regularly.

How will email be managed?
Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools in neighbouring towns, regions and in different continents can be created.

The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.
In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.
The use of email identities such as *john.smith@school.sandwell.sch.uk* generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify both a student's full name and their school. For Key Stage 1 and foundation stage pupils, whole class or project email addresses should be used.
• Pupils may only use approved email accounts. (School learning platform – Openhive)
• Pupils must immediately tell a teacher if they receive offensive email.
• Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
• Access in school to external personal email accounts may be blocked.
Children will annually review their use of email and alongside curriculum learning agree to the User Agreement to state they understand and agree to the terms of use of their school email account.

How will published content be managed?
The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. The school may also publish information for parents and pupils via the schools learning platform, this will be available to subscribed and approved users only.
• The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?
Children may only have their images used if approved by parents or guardians. This information will be stored in the school office and should be consulted before images are produced, in keeping with school policy. Images that include pupils will be selected carefully and will not provide material that could be reused.
• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
• Pupils work can only be published with their permission or the parents.

How will filtering be managed?
The school will work with the local authority, Becta and the Schools Broadband team to ensure that systems to protect pupils are reviewed and improved.
• If staff or pupils discover unsuitable sites, the URL must be reported to the Computing Co-ordinator.

• The school's broadband access will include filtering appropriate to the age and maturity of pupils.
• Senior staff and the Computing Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
• Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
• The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

Policy Decisions

How will Internet access be authorised?
The school will allocate internet usage access as appropriate. Normally most pupils will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission will be required for Internet access in all cases — a task that may be best organised annually when pupils' home details are checked and as new pupils join.
• The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
• All staff must read and sign the 'Staff User Agreement' before using any school ICT resource.
• At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
• Parents will be asked to sign and return a consent form for pupil access.
• Parents will be informed that pupils will be provided with supervised Internet access

How will risks be assessed?
As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the issue that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system.

How will Online Safety complaints be handled?
Parents, teachers and pupils should know how to use the School's complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.
A minor transgression of the rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or Online Safety Coordinator.
• 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.

• All Online Safety complaints and incidents will be recorded by the school — including any actions taken.
• Parents and pupils will work in partnership with staff to resolve issues.

How is the Internet used across the community?
Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, and supermarket or cyber café. Ideally, young people would encounter a consistent policy to Internet use wherever they are.
In community Internet access there is a fine balance to be achieved in ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools.
• The school will attempt to liaise, where appropriate, with local organisations to establish a common approach to Online Safety.
• The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyberbullying be managed?
Cyberbullying can be defined as *"The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone"* DFE 2007.
It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.
There will be clear procedures in place to support anyone affected by Cyberbullying.
• All incidents of cyberbullying reported to the school will be recorded in the bullying incident report.
• There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
• The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary
• Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.

- Internet access may be suspended at school for the user for a period of time.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms and learning environments be managed?

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils, parents as well as support management and administration. It can enable pupils and teachers to collaborate in and across schools, can share resources and tools for a range of topics, create and manage digital content and pupils can develop online and secure e-portfolios.

• Pupils/staff will be advised on acceptable conduct and use when using the learning platform.

• Only members of the current pupil, parent/carers and staff community will have access to the LP.

• All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

• When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

• Any concerns with content may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The material will be removed by the site administrator if the user does not comply.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of SLT before reinstatement.
  - A pupil's parent/carer may be informed.

How will the policy be discussed with staff?

ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion of the school Online Safety Policy.

The Online Safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and pupils, the school will implement User Agreements.

Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is 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.

• Staff training in safe and responsible Internet use both professionally and personally will be provided annually.

How will parents' support be enlisted?
Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
• A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
• Parents will be requested to sign an Online Safety/internet agreement as part of the Home School Agreement.
• Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
• Interested parents will be referred to organisations listed in section "Online Safety Contacts and References."

E-Safety Contacts and References Becta:
www.becta.org.uk/safeguarding
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation: www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk

St Martins C of E Primary School
Staff, Governors and Visitors
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher/ school eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils or parents.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the Head Teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken using school equipment, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or that of others, or the school into disrepute. School equipment should not be used to access social networking sites (E.g Facebook).
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school. I understand that a breach of the above would be a serious offence and could lead to disciplinary action.

Signature

……

……Date ……

Full Name ……(printed)

Job title . . . . . .

Online safety agreement form: parents/carers

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, School Website, e-mail and other ICT facilities at school.

I know that my daughter or son has signed an online safety agreement form and that they have a copy of the 12 'rules for responsible ICT use'. These rules have been discussed in class with their teacher.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: _____

Date: ___/___/___

Further information for parents on Online Safety can be found on the School Website.

Online safety agreement form

Keeping safe: stop, think, before you click!

Pupil name: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me. ☐

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules. ☐

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. ☐

I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer. ☐

Pupil's signature _____

Date: ___/___/___

Keeping safe: stop, think, before you click

12 rules for responsible ONLINE use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.