St Mary & St Paul's
CE Primary School

Online Safety Policy

October 2024

"Life in all its fullness through
Learning and Love"

This policy will be reviewed regularly and re-presented to The Governing Body as appropriate if significant changes are made.

To be reviewed: Every two years

Reviewed by:	S Reeve	Date: 19th October 2024
Headteacher Signature:	P Brooksbank	Date: 19th October 2024
Chair of Governors Signature:	Norma Garvey	Date:

Vision and Values

The school's vision and mission statement underpins the high standards of behaviour expected at all times at St Mary & St Paul's CE Primary.

'Life in all its fullness through Learning and Love'

This policy should be read in conjunction with the Anti-Bullying Policy, Behaviour Policy, Acceptable Use Policy (see appendix) and the Safeguarding & Child Protection Policy.

Online Safety is an important part of keeping children safe at St Mary & St Paul's CE Primary School. It covers all electronic media and we constantly strive to protect and educate our pupils in the digital world we live in. It is embedded into our school curriculum, particularly in Computing and PSHE lessons. Pupils are taught how to stay safe and behave appropriately online.

We aim to tackle any Online Safety issues by trying to prevent it from occurring in the first place, and by tackling it consistently, fairly and effectively whenever it does. We are committed to promoting a safe environment online where children can learn and play, as well as communicate sensibly, while also being aware of the risks and dangers.

At St Mary & St Paul's, we take pride in the teachings of our unique school values that underpin and promote the British fundamental values where British law, democracy and a mutual respect and tolerance for those of other faiths, cultures and beliefs is embedded through all areas of the curriculum. Pupils are encouraged to be independent learners, constantly making choices, within a safe and supportive environment. Developing their self-esteem and self- confidence is very important. Pupils are encouraged to understand their personal freedoms and are taught how to use these rights to best effect.

Areas of Risk

The main areas of risk for our school community can be summarised as follows:

Content

• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.

•Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.

•Hate sites.

•Accessing social media sites inappropriate for primary aged children

•Content validation: how to check authenticity and accuracy of online content.

Contact

•Grooming.

•Cyber-bullying in all forms.

•Identify theft (including hacking social media profiles) and sharing passwords.

Conduct

•Privacy issues, including disclosure of personal information.

•Digital footprint and online reputation.

•Health and wellbeing (amount of time spent online).

• Sending and receiving of personally intimate images (nudes or semi-nudes) also referred to as SGII (self- generated indecent images).

•Copyright (little care or consideration for intellectual property and ownership - such as music and film)

The policy applies to all members of St Mary & St Paul's CE Primary School community (including staff, students, volunteers, parents/carers visitors, community users) who have access to and are users of school/ academy computer and communication systems, both in and out of St Mary & St Paul's CE Primary School.

Role and Responsibilities

Leadership Team

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community.

- The Leadership Team are responsible for ensuring that the Computing Subject Leader / DSL and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

- The Leadership team should be trained in Online Safety issues and be aware of the potential child protection issues.

- The leadership team will liaise with school ICT technical staff and receive reports of Online Safety incidents and will log this information and use it to inform future Online Safety developments.

- That staff receive yearly update training and regular updates regarding online risks

Computing Subject Leader

As part of their role, the Computing Subject Leader will take day to day responsibility for Online Safety issues and having a leading role in establishing and reviewing Online Safety policies/documents. In addition, they will:

- ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.

- promote an awareness and commitment to Online Safety

- ensure that Online Safety education is embedded across the curriculum.

- provide training and advice for staff and parents.

- liaise with the Local Authority and relevant staff in our Connect network group.

- liaise with school ICT technical staff and receive reports of Online Safety incidents. They will log this information and use it to inform future Online Safety developments.

•record and review all incidents relating to extremism in order to establish whether there are any patterns of extremist groups targeting the school and whether current procedures are robust enough to deal with the issue.

Local Authority

It is the roles of the ICT team at the Local Authority to ensure that:

- reasonable systems are put in place to ensure that the network and related infrastructure is as secure as possible.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with Online Safety technical information in order to effectively carry out his Online Safety role and to inform and update others as relevant.
- equipment is protected adequately against threats such as hacking and viruses.
- the network infrastructure is monitored regularly and consistently.

Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- they have an up-to-date awareness of Online Safety matters and of the current school / academy Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement
- they report any suspected misuse or problem to the Headteacher / Senior Leader / Computing Coordinator for investigation /action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- e-mails sent to parents/guardians to be on a professional level and sent through maryandpaul@knowsley.gov.uk

- they are aware of those students who may be targeted or exposed to harmful influences from violent extremists via the internet. Students and staff are warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies. All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate. All incidents should be reported to the DSL and Prevent / Channel via Knowsley MASH.

Governors

To enable the Governing Body to carry out its duties in promoting high standards of education and achievement, governors need to be fully informed about the standards in Online Safety as well as priorities for development. Governors are kept informed in the following ways:

- The Headteacher reports to governors termly on progress towards objectives within the school improvement plan.
- The governors are given the opportunity to approve the Online Safety Policy and review the effectiveness of the policy.

Safeguarding Designated Persons

Any safeguarding designated person should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

Parents

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of Computing than their children. The school will therefore take every opportunity to help parents understand these issues through the school website, parent evenings and newsletters. Parents may also be invited to attend Online Safety workshops.

Parents/Guardians will be responsible for:

- supporting the school in promoting Online Safety and endorsing the Parents' Acceptable Use Agreement (see Appendix 2) which includes the pupils' use of the Internet and the school's use of photographic and video images.
- reading, understanding and promoting the school Pupil Acceptable Use Agreement with their children.

- consulting with the school if they have concerns about their children's use of technology.
- Parents are invited to sign the Parental Acceptable Use document.

Pupils

It is important that all pupils at St Mary & St Paul's CE Primary school:

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• will be expected to know and understand policies on the use of mobile devices and digital devices. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's / academy's Online Safety Policy covers their actions out of school, if related to their membership of the school. Pupils are invited to sign the Acceptable Use document for children.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

•Policy to be posted on the school website with hard copies available from school on request.

•Policy to be part of school induction pack for new staff.

•Acceptable use agreements discussed with pupils at the start of each year.

•Acceptable use agreements to be recorded by the office and kept in teacher files.

When using communication technologies, the school considers the following as good practice:

•The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

•Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

•Any digital communication between staff and pupils (on iOS applications such as Tapestry / Google Classroom) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.

•Students / pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
•Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Approaches to Teaching and Learning

Online Safety is embedded into the curriculum and is covered through Computing and PSHE objectives. Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Pupils will be expected to know school rules and understand school policies for bullying and behaviour, this is reinforced through Safer Internet Sessions each half term. Pupils should understand the importance of adopting good Online Safety practice when using digital technologies out of school.

Handling complaints

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

•Interview with teacher/ Computing Subject Leaders/ SLT / Headteacher;
•Informing parents or carers;
•Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including online homework];
•Referral to LA / Police.

Our Deputy Headteacher acts as the point of contact for any complaint. Any complaint about staff misuse is also referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The Online Safety policy is referenced from within other school policies:

- The school has Computing and PSHE subject leaders who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online Safety policy has been written by the school Computing and PSHE subject leaders and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Planning and Organisation

Online Safety should be focused upon in all areas of the curriculum and staff should reinforce Online Safety messages during computing lessons. The Computing Subject Leaders have a clear, progressive and up-to-date Online Safety education programme as part of the Computing curriculum/Online Safety curriculum. This covers a range of skills and behaviours appropriate to their age and experience.

In the Foundation Stage, pupils are taught to not give out any personal information on the internet. They are told to tell a teacher or parent if anything they see on the internet makes them feel uncomfortable. At St Mary & St Paul's CE Primary School, we do expect children of this age to be supervised whilst using the internet. Reception pupils take part in the school "Safer Internet Week" using age appropriate CEOP resources.

In Key Stage One, pupils begin to understand what personal information is and who you can share it with. Children begin to recognise the difference between real and imaginary online experiences. They are taught to keep their passwords private and make sure that an adult knows what they are doing online. Teachers model appropriate online behaviour when communicating with others.

There are four key messages taught at Key Stage One:

- People you don't know are strangers. They're not always who they say they are.
- Be nice to others on the internet, like you would on the playground.
- Keep your personal information private.
- If you ever get that 'uh-oh' feeling, you should tell a grown-up you trust.

In Key Stage Two, themes taught in Key Stage One are built upon. In addition, pupils are made aware of online experiences which could cause potential danger, e.g. use of social networking, gaming sites and downloading or installing new applications. Links are made between inappropriate sharing of personal information and the dangers this can pose in the real world. Relevant resources from CEOP, Ineqe, Childnet and SWGfL are used during "Internet Safety Week" and other resources can be accessed throughout the year on the school website. In Key Stage Two, children also develop their research skills, especially through use of their iPads. They are taught about plagiarism and the need to upload copyright laws.

Resources

Online Safety resources are mainly online safety websites – provided by the ICT / Computing coordinator. Information about new resources/websites are communicated to staff via email.

Inclusion

At St Mary & St Paul's CE Primary we believe that all our children should be given the opportunity to achieve as well as they can in everything they do.

Acceptable Use of Personal Equipment – Children

Children have all read and signed the acceptable use of equipment document (copy available on request)

Use of Facebook / Social networking sites

Children are not permitted to use social networking sites on school premises. Both on computers or mobile devices. Children are also reminded of minimum age guidelines for various social networking sites, as part of their Online Safety lessons.

Use of Mobile Phones

Mobile devices must be switched off and handed to Year 6 class teacher at the start of each day. Children are not allowed to take mobile phones on any school residential trip. Mobile phones brought into school are entirely at the staff member/ visitors' own risk. St Mary & St Paul's CE Primary School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Where parents or students need to contact each other during the school day, they should do so only through the school's telephone.

Email

Children may have access to messaging systems on iOs applications such as Google Classroom, though all messages must be approved by the class teacher before the messages go live. Other messaging or e-mail solutions may be used when appropriate for a particular year group.

Cyber-Bullying

Safer Internet Week is held annually with up to date Online Safety guidance. The school website has links to cyber-bullying advice. Incidents of cyber-bullying are dealt with by leadership team and communicated to parents where necessary.

Acceptable Use Policy (AUP)

The AUP is distributed to all pupils on joining the school and signed by parents/guardians. The AUP will be reviewed during KS2.

Acceptable Use of Personal Equipment - Staff

Use of Facebook / Social networking sites

Staff are not permitted to access Facebook or most other social networking sites from a school computer whilst on school premises. Staff are permitted to use Twitter on school computers for educational purposes and networking. Social networking sites can be accessed on a personal handheld device at break times only. Staff are allowed to use the school Twitter account.

Staff must check the school GDPR document to check the levels of photograph permissions for their children.

Use of Mobile Phones and other personal mobile devices

See Mobile Phone Policy. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode when in classrooms. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally- owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Staff will be issued with a school phone where contact with students, parents or carers is required.

If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the designated staff area of the school, e.g. staffroom, an office area.

If any staff member has a family emergency or similar and is required to keep their mobile phone to hand, prior permission must be sought from a senior manager and the mobile phone should be stored in an agreed location.

Some staff do use mobile phones for access to Google Chat / Meet / Classroom and Drive – as part of the school working practices. SLT also will use their mobile phones to add to the school twitter account (@stprescot)

Use of Cameras

Images of pupils and/ or staff must only be stored on computers/drivers owned by the school. Images will not be distributed outside the school network (e.g. Website/local press/school app) without the permission of the parent/ carer, member of staff or Headteacher.

Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such image. Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website. (see School GDPR Policy and procedures)

Email

Emailing is used as one of the many ways we communicate with each other at St Mary & St Paul's CE Primary School. However, the system should be used responsibly and staff should always act in a professional manner when using the email system. Members of staff should not feel obliged to reply to any emails sent to them in the evenings or at weekends and equally staff should not expect a reply from colleagues outside school hours. Staff are reminded of this at the start of the school year.

Acceptable Use Policy (AUP)

The AUP is distributed to all staff during on starting school. The AUP will be reviewed annually.

Incident Management

In this school:

- there is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support will be actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with Online Safety issues
- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in Online Safety within the school.
- parents / carers are specifically informed of Online Safety incidents involving young people for whom they are responsible.
- we will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Computing Subject Leader, or Leadership Team.
- all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Computing Subject Leader.