ST. MARTIN'S
CE Primary School

St Martin's CE Primary School Online Safety Policy

May 2023

1. Policy statement
Our Online Safety Policy should be read in conjunction with other related school policies and documents. In particular, this document will be used in conjunction with the Frays Academy Trust Behaviour Policy, Safeguarding Policy, ICT Usage Policy, Anti-Bullying Policy and the Blended Learning Policy.

2. Policy aims
The schools within the Frays Academy Trust provide a rich and broad approach to the use of technology to support pupils' learning. We aim to ensure that children's learning is enhanced by the use of such technology, and that children are equipped with the skills and knowledge to use technology appropriately and responsibly. We believe that children must be taught to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. Information and Communications Technology (ICT) in St Martin's CE Primary School covers a wide range of resources including web-based and remote learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Above all, we aim to ensure that all children are protected from harm when using the internet.
Currently the internet technologies children and young people use both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

We ensure that all members of the school community understand their role in keeping children safe online.

3. The role of the Senior Leadership Team. (E-safety coordinator or ICT coordinator)
The Headteacher has overall responsibility for e-safeguarding all members of the school community, though the day to day responsibility for e-safeguarding will be delegated to the DSL.

The Headteacher and senior leadership team are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.

The role of the Senior Leadership Team and ICT Leader include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated policies
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored
- Ensuring that any Online Safety incidents are effectively investigated and resolved
- Keeping personally up-to-date with Online Safety issues and guidance
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors
- Liaising closely with the school's Designated Safeguarding Lead to ensure a coordinated approach between Online Safety and safeguarding

4. Policies and Practices

This section of the Online Safety Policy sets out the school's approach to Online Safety along with the various procedures to be followed in the event of an incident.

4.1 Security and data management

All data in the school is kept secure, in accordance with the Online Safety Policy and ICT Usage Policy. Staff are made aware of this as part of induction, and through regular training. The ICT Usage Policy should be signed by staff annually.

4.2 Use of mobile devices

The use of mobile devices such as iPads, Chromebooks, laptops, offers a range of opportunities toextend children's learning. Staff are aware that some mobile devices e.g. mobile phones, game consoles or smart watches can access unfiltered internet content and therefore may pose a risk to children.

- Mobile devices are not encouraged to be brought into school by children.
- Any phones brought to school by children who walk home alone and require them for safety reasons should be turned off, locked away during the school day and not used by children whilst on school property.
- Children must have a permission slip to bring in a mobile phone.
- Children are not permitted to bring games consoles or personal tablets into school.
- Children are not permitted to wear smart watches that are able to connect to the internet or have the capacity to take photographs.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure, school Facebook or display.

- At school photographs and videos of pupils and staff are regarded as personal data, and the school has written permission for their use from their parents or carers
- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used
- The parental/carer written permission is obtained by the school office but the parents have a right to change this at any time
- The staff and pupils aware that full names and personal details will not be used on any digital media, particularly in association with photographs
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs. Parents /carers are however reminded not to publish these images on social media if they contain images of children who are not their own
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils
- Staff are encouraged not to store digital content on personal equipment
- Staff do not use their own cameras or smartphones for the purposes of taking photos or videos
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks. All

school devices that hold personal data (as defined by the Data Protection Act 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately.

Email

- All users have access to the London Grid for Learning service as the preferred school e- mail system.
- All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.
- This email system should be used by staff in accordance with the ICT Usage Policy.
- We use the in-built software that aims to prevent any infected email to be sent from the school, or to be received by the school.

Social Networks

Social Network sites should be used by staff in accordance with the ICT Usage Policy and the Social Media Policy.

Apps

Smart phones are increasingly being used by younger children today. These allow children a range of access to people around the world, allowing them to publish pictures, communicate and share information. Staff need to raise awareness of the risks involved to children and educate them on the correct usage and guidance.

- Children should be aware of the ages required to use different platforms such as;
    - Snapchat
    - Tik Tok
    - Youtube
    - Facebook
    - WhatsApp
    - Fortnite
- Adults must not communicate with pupils using any apps.
- Pupils should be aware of the potential dangers of using apps and have guidance on how to report any misuse or concerning content.

E-Learning Platforms

Schools use sites including (but not limited to) Times Table Rockstars (TTRS) and Spelling Shed. Other suggested sites for pupils to use are Top Marks and BBC bitesize.

- All children will be given access to, TT Rockstars , Teams but SLT will have access and admin rights across the learning platforms.
- Where images of pupils are shared via online learning platforms, such as Tapestry, members of staff will ensure that written consent has been given by parents.
- Passwords are issued to the children and they are taught not to share their password, and the reasons for this.
- Pupils are taught to use these communication tools in a responsible way in conjunction with the e-safety curriculum.
- Teachers know how to use and monitor programmes used across the classroom. Teaching staff will have administration rights within their own class.
- Teachers will report any concerning comments, images or blogs to the DSL in accordance to safeguarding procedures.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Accounts are kept historically on the server however are made inactive by the administrator. This is

completed annually.

Others
The School will adapt/update the Online Safety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

4.5 ICT Usage Policy
Our ICT Usage Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

Our ICT Usage Policy is used for staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology.

4.6 Dealing with incidents
Any e-safety concerns will be reported and dealt with in accordance with the Child Protection Policy and Behaviour Policy.

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Staff will not personally investigate, interfere with or share evidence to avoid inadvertently committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to appropriate agencies.
Examples of illegal offences are:
- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content

Incitement to racial hatred

Inappropriate use
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The Senior Leadership Team will decide what constitutes inappropriate use and the sanctions to be applied in line with the Behaviour Policy.

All complaints of internet misuse will be investigated by the Headteacher and a record will be kept. Examples of inappropriate use are:
- An image of a pupil is published without permission
- An explicit, offensive or inappropriate message is sent on a school platform between pupils
- A child publishes something on their school profile which is deemed unacceptable
- A report of bullying via school platforms is made
- A child has accessed material online, including images, that is not age appropriate
- Information about a pupil is shared online without permission

Where the complaint/concerns raise behavioural concerns, it will be reported to a Senior Leader. If it is determined that a pupil's behaviour was deliberate, this will be dealt with in accordance with the school behaviour policy. A log will be kept of all complaints of internet misuse by pupils. Parents will be informed, and staff will work in partnership with the parents and pupil to resolve the issue.

If a complaint of inappropriate use is made by a pupil against another pupil, the following steps will be taken:

- The pupil should be reassured they have done the right thing by telling a member of staff
- It will be ensured that the pupil understands the behaviour was inappropriate, and they should not copy or retaliate the behaviour
- Actions will be taken to contain the incident, for example if the action relates to an inappropriate post, this will be screenshotted by a member of SLT, logged, and then the original content removed
- Posts or images published to external websites will be reported and removed
- The parents of both pupils will be informed
- Actions will be taken in partnership with parents to resolve the issue and ensure it does not take place again in the future
- All incidents of cyber bullying will be recorded, investigated and dealt with as bullying, according to the Behaviour Policy
- If an incident raises issues of peer on peer abuse, the DSL will act in accordance with the Child Protection Policy

Where the complaint relates to the inappropriate use of technology/internet by a member of staff, this will be referred to the Headteacher.

It is known that children may be at risk of harm when using the internet. This can include:

- Online relationships
- Fake profiles
- Grooming
- Sexting
- Child Sexual Exploitation
- Child Criminal Exploitation
- Sexting
- Live streaming on devices/platforms such as Xbox, Playstation, SnapChat, TikTok, Discord
- Online gambling

Where a complaint/concern raises child protection concerns, it will be reported through the usual channels using the school's safeguarding reporting process and a DSL/DDSL will act in accordance with the school's Child Protection Policy.

The following actions may be taken where necessary to protect a pupil from harm:

- Discussion with child
- Report to DSL
- Escalate to Safer Families Hub
- Report incidents to associated websites
- Support children and their families in stopping contact with harmful individuals online
- Support children and their families in blocking harmful individuals online
- Support children and their families in capturing evidence of online abuse
- Inform the police
- Address the issues in school, through support, education and parent awareness

School staff will never share, download or view images of children in the context of an investigation. If staff accidentally view images of children because they have been shown the image without asking to see it, staff will report this to the DSL and Headteacher immediately.

5. Infrastructure and Technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband

connection, filtering and virus protection are in place.

Pupil access

- The children are supervised by staff when accessing school equipment and online materials.

Passwords

- All users of the school network have a secure username and password.
- The administrator password for the school network available to the Headteacher and other nominated senior leader is kept in a secure place (this must be authorised by the Executive Headteacher).
- Staff and pupils are reminded of the importance of keeping passwords secure. All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords will only be changed if the need arises.

Software/hardware

The school has legal ownership of all software.
The school has an up to date record of appropriate licences for all software

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The SLT is responsible for managing the security of the school network. School ICT systems capacity and security will be reviewed regularly. Sophos anti-Virus protection is updated regularly.
- The safety and security of the school network is monitored on a regular basis. System security is overseen by our technicians.
- The school systems are kept up to date in terms of security e.g computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the SLT
- The school encourages staff not to use removable storage devices on school equipment e.g. encrypted pen drives.
- The school encourages teachers to follow Online Safety/ICT Usage policy guidelines when using laptop for personal/family use
- If network monitoring takes place, it is in accordance with GDPR
- All internal/external technical support providers are aware of school's requirements / standards regarding e-safety
- The SLT and ICT Leader are responsible for liaising with/managing technical support staff.

6. Teaching and Learning

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

1. How to evaluate what they see online
2. How to recognise techniques used for persuasion
3. Acceptable and unacceptable online behaviour
4. How to identify online risks
5. How and when to seek support

6.1 e-Safety Curriculum

- Internet use will enhance learning
- E-safety is embedded within the computing curriculum, as well as being taught explicitly in Computing and PSHCE lessons. Please note that St Martin's CE Primary School follow the Kapow Online safety
- The school will provide opportunities within a range of curriculum areas to teach e-Safety. E-safety lessons can be taught at any time, depending on the needs and requirements of a class or cohort of children.
- All children, including those with educational needs, have access to the E-Safety curriculum.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues. Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Early Years

In the Early Years, we recognise that children's natural curiosity, and the increasingly online nature of our daily lives, leads children to be using devices from an increasingly young age. We aim to support children in investigating how technology impacts their own lives, as well as develop pupil's understanding of how to be safe online. Children will be supported to develop early ICT skills, which will become essential to the skills they need in later life as Global citizens and members of the wider community. Through the teaching of ICT in the Early Years, we aim to foster critical thinking skills, problem solving, imagination and creativity in children.

Children will be taught to:

- Understand the importance of using devices only with the guidance and supervision of a trusted adult
- Understand that they should tell an adult if they feel unsafe because of something they saw online
- Recognize examples of technology that they come across in the daily lives, such as at home or at school
- Understand how technology can be used to create links to our communities and the wider World
- Begin to experiment with a range of ICT devices, including tablets and computers, with the help of a trusted adult
- Switch a simple device, such as a tablet, on and off
- Use age appropriate software for a purpose – for example to create a picture using Paint
- Begin to understand the concept of "logging in" and do so with support

How our Computing curriculum meets National Curriculum objectives for eSafety:

Each year group covers different aspects of e-safety. See Appendix 1 to find out what objectives are covered in each year group.

How does RSE relate to eSafety?

According to the RSE guidance set out by the Government, by the end of Key Stage 2, pupils should know:

- that people sometimes behave differently online, including by pretending to be someone they are not.

- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.

Through our RSE curriculum children in all year groups learn about how to stay safe online, the dangers ofthe internet and online relationships.

6.2 Use of ICT across the curriculum

- ICT is used to enhance learning across the curriculum
- Children are signposted to appropriate search engines and website by teachers
- Any websites or links used are vetted by staff prior to the lesson taking place
- Children's use of ICT, particularly the Internet, is monitored by staff throughout the lesson
- Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:
  - Where does this organisation get their information from?
  - What is their evidence base?
  - Have they been externally quality assured?
  - What is their background?
  - Are they age appropriate for pupils?
  - Are they appropriate for pupils' developmental stage?

6.3 Use of ICT for home learning

- Homework given by teachers may require the use of ICT
- Home learning may be set online in the event of a school closure
- Staff will use Teams to set tasks and provide home learning resources
- Staff will use Teams to signpost children to other websites or platforms that may support their learning
- Any websites, resources or platforms signposted will be vetted by staff prior to the content being uploaded
- Any websites, resources or platforms signposted will be age appropriate and in line with the school's vision and ethos
- Any websites, resources or platforms signposted will be GDPR compliant
- Any and all pupil activity on Teams will be regularly monitored by staff, and any concerns reported to the SLT to be followed up
- Staff will communicate with children on Teams by means of public posts, blogs, forums or comments
- Staff will not enter into private messaging with children on Teams or any other platform, including social media. If a staff member receives a private message on Teams, a second member of staff will be included in the response.
- Parents will receive appropriate support in enabling their child to access home learning

When asking children to complete home learning online, the school will ensure that pupils develop an understanding of the importance of the ICT Usage Policy and are encouraged to adopt safe and responsible

use of ICT both within and outside school. Pupils are reminded of safe Internet use e.g. classroom displays, e-safety rules, E-Safety Day, E-Safety learning modules on Teams.

When asking children to complete home learning online, the school will ensure that children have very clear reporting routes in place so they can raise any concerns whilst using online platforms, for example, using the 'whistle' function on Teams, or sending their teacher a 'mail' message (although the teacherwill not respond directly). Schools will also signpost children to age appropriate practical support, such as Childline.

Remote learning

During times of remote learning, staff members are responsible for:

- Reporting any health and safety incidents to the health and safety officer and asking for guidance as appropriate.
- Reporting any safeguarding incidents to the DSL and asking for guidance as appropriate.
- Taking part in any training conducted to meet the requirements of this policy, including training on how to use the necessary electronic equipment and software.
- Reporting any dangers or potential dangers they identify, as well as any concerns they may have about remote learning, to the Headteacher.
- Reporting any defects on school-owned equipment used for remote learning to an ICT technician.
- Adhering to the Staff Code of Conduct at all times.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.
- The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During times of remote learning, all staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.

- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

7 Online Safety awareness in our community

7.1 Staff awareness

- There is a programme of formal e-safety training for all staff to ensure they are regularly updated on their responsibilities.
- The SLT and ICT Leader provides advice/guidance or training to individuals as and when required.
- The Online Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and ICT Usage Policy.
- Regular updates on Online Safety Policy, ICT Usage Policy, curriculum resources and general e-safety issues are discussed in staff/team meetings.

7.2 Parent/carers' awareness

The school offers opportunities for parents/carers and the wider community to be informed about e-safety, including the benefits and risks of using various technologies. For example through:

- School newsletters, homework books, school website, Teams and other publications.
- Promotion of external e-safety resources/online materials.

To help and support the school in promoting eSafeguarding:

· To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.
· To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
· To model safe and responsible behaviours in their own use of technology.
· To consult with the school if they have any concerns about their children's use of technology.

7.3 Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for Safeguarding, are kept up to date. This is through discussion at Governor meetings and Governor training.

Governors must read, understand, contribute to and help promote the school's eSafeguarding policies and guidance, specifically:
· To develop an overview of how the school ICT infrastructure provides safe access to the internet.
· To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
· To promote and ensure safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safety activities.
· To ensure appropriate funding and resources are available for the school to implement its e-safety strategy.

<u>Concerns over Excessive use of Technology by Pupils</u>

As a school we understand that excessive use of the internet and technology by children, can significantly impact their mental health and well-being. To mitigate this risk, pupils will be supported in developing their

understanding of these risks through the e-safety curriculum. Staff will receive training about e-safety specific to children, alongside regular Safeguarding training, and training regarding the mental health and well-being of children.

If a concern is raised about a pupil's excessive use of the internet, the following steps will be taken:

- The concern should be reported to a DSL or DDSL
- Parents will be informed, and possibly supported by the Learning mentor/ MET police
- Parents will be supported in managing and monitoring their child's use of ICT
- Pupil will be supported by the Learning Mentor