St Martin's C of E Primary School

Online Safety Policy

Jan 2025
Review 2026

Contents

Introduction

At St Martin's C of E, we aim to provide children with exciting and engaging learning experiences across all areas of the curriculum. The growth of technology and the access to the internet and the digital world is forever growing especially for children and young adults. In recent times, both children and adults have had to (and are continuing to) adapt to using technology more frequently for a range of different reasons that they may not have used it for before. Therefore, it is more important than ever that we continue to ensure children use a wide range of technology in and out of school to its full potential and in a safe way. Even though we have had to adapt to using technology in new ways and have relied upon it more than ever before in recent times, it is key to highlight to children, families and staff that it is equally important to balance time online and offline.

We aim to encourage and allow children to further advance their skills. This is done by providing a safe environment for children, which allows them to explore devices and the digital world safely, encouraging and motivating them to become a positive, constructive and reflective "digital citizen". It is vital that children, as well as their families, school staff and other stakeholders associated with children are aware of risks online and procedures and the safeguarding, we have in place at St Martin's. This allows us to work together in partnership to encourage and ensure our children live well-balanced digital lives.

In addition to this, we support them in their use of technology and in developing their understanding of the digital world and how it can have a great positive impact on our lives. However, we also must support them in understanding some of the negative implications the use of technology can have and the potential risks we may face if we use it incorrectly. We do this in a way that promotes their knowledge of how to avoid risks and in the event of being faced with them they are confident to know how to deal with these issues, what to do in different situations, who to contact or report to, etc.

Our delivery of online safety at St Martin's strives to educate children, parents, staff and governors on a regular basis. This allows individuals to use software, applications, hardware and other links to technology and a digital world effectively and demonstrate clear knowledge of how to be safe online. In addition to this, it should also provide children with opportunities to develop a passion for Computing as a subject and use technology to further their love for learning in all curriculum areas. Livingstone Et Al, who is referenced in the UKCCIS's literature review (prior to 2023), suggests that "the more and better-quality children's access (to technology and having opportunities to use online services), the deeper and more diverse are their online activities." Therefore, we want our children to be able to broaden their use of technology and identify when using technology and being online can support their learning, further their knowledge and develop their passions yet also be able to identify when it is best to use an alternative that does not require the use of technology.

The Online Safety overview (appendix A) shows how Online safety is taught throughout the school using age-appropriate resources and objectives to ensure that the curriculum is taught effectively and accurately. Staff use this alongside the "Education for a Connected World", and other resources/documents to support with key vocabulary and to gain understanding of what is expected regarding their online safety education at each milestone

of their education within our school. In addition to this, we understand that some children may be more vulnerable than others online. Therefore, we take this into account when considering planning by thinking about the needs of each individual child and the resources we may choose to use.

All staff, including governors are trained and reference relevant and informative documents such as the "Teaching Online Safety in Schools" document and the most up to date version of "Keeping Children Safe in Education" to support their own knowledge, planning and teaching of the subject. They also understand the importance of drawing on other areas of the curriculum while planning and teaching such as PSHE, RSE and SMSC.

This policy is supported by several other policies that work alongside to safeguard children, particularly with links to being online. In addition to this, it is also supported by the Staff Code of Conduct. These aim to protect the safety of users and the school by minimising risks and making users aware of what is expected in terms of the use of technology and accessing the digital world. It also clearly states what is expected of the user, allowing them to avoid infringement. This policy, as well as the Staff Code of Conduct should be read alongside our Safeguarding and Child Protection Policy, Mobile Phone Policy, Computing Policy, Remote Learning Policy, Acceptable Use Policy (AUP). This policy and the Acceptable Use Policy are in reference to both fixed and mobile internet, technologies provided by school (such as PCs, iPads, whiteboards etc.) and technology owned by parents, pupils, staff, governors and any visitors to the school that wish to use digital devices.

As pupils learn new skills linking to the digital world in Computing and across our curriculum, both at school and at home, we believe parents, children, staff and governors should be aware of potential risks to consider.

What are the risks?

-Receiving and accessing inappropriate content.
-Predation and grooming.
-Sharing/distributing of personal images without consent.
-Requests for/loss of/unauthorised access to personal information (GDPR).
-Viewing 'incitement' sites.
-Bullying and threats.
-Identify theft.
-Publishing inappropriate content.
-Online gambling.
-Misuse of computing or digital systems.
-Publishing personal information.
-Hacking, security breaches and cybercrime.
-Corruption or misuse of data.
-Self-hate and harm content.
-Cyber bullying.
-Being subject to Fake News.
-Placed in situations that impact wellbeing and mental health.
-Upskirting.

-Radicalisation and Extremism.
-Sexting.
-Child-on-child abuse.
- Sexual harassment, exploitation, violence, etc.
-Consensual and non-consensual sharing of images, media, e.g. nude and semi-nude images.
-Initiations/Hazing including online elements.
-Elements linking to Child Criminal Exploitation (CCE).
-Potential negative impacts on mental health.

Many of these issues are reflected in "real world" situations away from the online portal. Therefore, this policy must be used in reference to other policies, such as the behaviour and anti-bullying policy, acceptable use policy, child protection and safeguarding policy, etc. It is important that we maintain the attitude discussed in KCSIE of "It could happen here."

It is also important to be aware of data collected, information regarding trends and other pieces of information that can support the teaching of online safety, safe use of equipment and technology.

Even though it is vital to consider and discuss risks it is equally important to think about the opportunities for using the internet, technology, etc alongside these. We must inform and teach children about potential risks (while also considering what is age appropriate and safe) so that they are able to apply their knowledge if they were to come across a similar issue independently, at home or in later life. UKCCIS highlights that positive experiences online as well as experiences that offer potential risk contribute to children's resilience and understanding of digital literacy.

An example of this may be at home children use a console to play online games with their friends. The positive is that it can be a tool to enhance communication, to work together and to develop a range of skills. Children should be taught the skills and information to ensure that they are taking precautions to do this safely. This could be playing with friends they know in real life, in a locked party, in a room in the house where an adult is present. A potential risk to this could be a stranger trying to add them. If this were to happen, they should then know who to report this to and what steps to follow to ensure they don't put themselves at risk.

Who will write and review this policy?

Summaries of the school's safety responsibilities are outlined below. This list will assist in developing a coordinated and effective approach to managing Online Safety issues.

Together, the senior leadership team and Computing coordinator will maintain the Online Safety policy, manage Online Safety training and keep abreast of local and national Online Safety awareness campaigns.

The school will review the policy regularly and revise the policy annually to ensure that it is current and considers emerging technologies for example changes to safeguarding e.g. KCSIE.

St Martin's will ensure that their filtering systems are up to date and monitored, alongside the

school's technical support partners.

To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse or concern need to be investigated and recorded on CPOMS.

The school will include regular opportunities to discuss and learn about Online Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report problems if they arise.

The Online Safety policy will be made available to all staff, governors, parents and visitors through the website and is available as a paper copy for free on request from the main office.

Why Internet use is important?

Developing effective practice in Internet use for teaching and learning is essential.

The purpose of internet use in school is to raise and enhance educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality and up to date internet access as part of their learning experience.

Pupils use the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security from the risks mentioned above.

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what internet use is acceptable and what is not and with be provided with clear objectives for internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils; Staff should guide pupils in 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.

Staff Responsibilities

Safeguarding Team and Computing Coordinator

- Ensure that the school are meeting requirements of expectations set out by the DFE in relation to meeting digital and technological standards in school.
- Organise appropriate training opportunities for staff including safeguarding, child protection training, online safety training, filtering and monitoring training and other training and CPD opportunities to support staff and children in the delivery, teaching and safeguarding of children when using technology and being active online.

- Ensure records are being recorded of any issues regarding online safety and actioned upon appropriately (CPOMS).
- Ensure the policy is reflected on constantly to ensure it meets requirements and act upon any changes, trends, etc.
- Feedback to be provided frequently to SLT and specifically the head, which can be shared with necessary groups e.g., staff, governors.
- Ensure training is provided to all staff and reflects up to date information.
- Provide staff and governors with cyber-security training.
- Ensure that filtering and monitoring standards are met and share information regarding online safety and filtering and monitoring with governors.
- Attend relevant and regularly updated training in online safety to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meet regularly with the online safety governor to discuss current issues, review incidents and filtering and monitoring logs and ensuring that filtering and monitoring checks are carried out
- Handle reports and decide whether to make a referral by liaising with relevant agencies.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- Review policies and documents about online safety.
- Liase with subject leaders and staff to ensure online safety is referenced and covered, evaluating and amending where necessary to ensure trends or issues that arise are addressed.
- Provide and organise training and advice for all stakeholders.
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners).

Other staff

There are several responsibilities, in reference to staff, that are essential to ensure Online Safety is delivered effectively throughout the school and to ensure pupils and the wider school community are motivated and encouraged to demonstrate the behaviour and knowledge of positive, critical thinking and constructive digital citizens.

These are:

- To receive and partake in appropriate safeguarding and child protection training, including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as referenced in KCSIE 2024.
- Knowing how to report and record an Online Safety incident (via SLT, CPOMS and Head Teacher).
- Be aware of responsibilities relating to safeguarding of children in the context of online safety and the digital world.

- Consider ways of supporting parents and children outside of school with their use of technology and access to the digital world.
- To ensure that online safety guidance is provided for parents. For example, in the form of website updates, parent workshops, newsletters, etc.
- Manage use of Outlook and 365 by staff, pupils and governors and any other platforms children have access to.
- Check websites, applications and digital links prior to showing/giving them to pupils.
- Switch screen of technology off immediately if anything inappropriate is visible and report to a member of the safeguarding team.
- Contact parents if required to do so to discuss issues.
- To understand and share with children (if required) that e-mail addresses, and any internet activity is monitored and can be explored further if needed.
- Incorporate online safety into their curriculum whenever possible and hold daily discussions, activities linking to online safety as advised in the online safety guidance.
- To promote and demonstrate evidence of being a positive, critical thinking and constructive digital citizen.
- Be aware of sites and support for children for example, CEOP.
- Do not take any photographs, videos, or digital recordings of pupils or place them on personal devices.
- Ensure that consent has been provided for children whose images are used on platforms such as the school website.
- Be aware that photos and videos taken must be strictly linking to learning and recorded on a school device (iPad, camera, computer, etc) only.
- Collect evidence of any incident and record on CPOMS.
- Have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- Understand that online safety is a core part of safeguarding
- Immediately report any suspected misuse or problem for investigation/action, in line with the school safeguarding procedures
- All digital communications with learners and parents/carers are 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
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements.
- Supervise and monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies regarding these devices
- Where lessons take place, activities or performances using live-streaming or video- conferencing, there is regard to national safeguarding guidance and local safeguarding policies (e.g. the guidance contained in the SWGfL Safe Remote Learning Resource)
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- Model safe, responsible, and professional online behaviours in their own

use of technology, including out of school and in their use of social media.

Partnership With Technical Support

At St Martin's C of E, we have a very close partnership with SIPS. The Computing coordinator and staff work with SIPS to meet requirements and put in place effective systems, which are put in place to reflect on our own school IT use and technology used.

SIPS:

- maintain filtering and monitoring systems
- support filtering and monitoring reports
- complete actions following concerns or checks to systems
- procure systems
- identify risk
- carry out reviews
- carry out checks

They ensure:

- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to SMT/DSL for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in school policies

How will Internet access be authorised and monitored?

Creating a safe and effective learning environment for learning in relation to IT includes a variety of key elements at St Martin's C of E:

- All staff must read and sign the 'Staff Code of Conduct' and Acceptable Use Policy before using any school computing resource.
- Staff, pupils and verified visitors can have access to school internet.
- An effective filtering and monitoring system is in place.
- Online Safety is delivered regularly to educate children, parents, staff and governors in a variety of ways and ensure their knowledge is up to date.
- Policies, such as this, and procedures are evident and clear.
- Online Safety incidents/issues are logged on CPOMS.

- Online Safety feedback as part of regular discussion during SLT meetings.
- Staff, pupil and governor e-mail can be monitored. Pupils' e-mail will be checked to ensure they are used correctly.
- Being aware that any communications with staff, pupils, parents or carers must be professional.

How will filtering be managed?

The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider.
- There are established and effective routes for users to report inappropriate content.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- The school will work in partnership with out IT Support to ensure systems to protect pupils are reviewed and improved.
- Senior staff alongside Business Manager (Mrs Michelle Judge) will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any unsuitable content or access (as well as online safety issues in and outside of school) will be noted via the CPOMS and be reported to SLT, our headteacher and SIPS.

How will monitoring be managed?

- Staff are aware that physical monitoring of pupil use of devices is required at all time.
- All devices using the school network at monitored using Senso. Alerts are sent to the headteacher, DSL and Business manager, who can see a live screen shot of the trigger. These are then reviewed and dealt with in line with our Filtering and Monitoring, Behaviour, Anti-Bullying and Safeguarding Policies.
- Genuine breaches are logged on CPOMS, with the next steps and any actions recorded.

Filtering and Monitoring Reviews

This will involve: Computing coordinator, DSL, Online Safety Governor, Staff, Learners, input from Parents, other agencies if possible. They will be involved in:

- The production/review/monitoring of the school Online Safety Policy/documents
- The production/review/monitoring of the school filtering policy and requests for filtering changes
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- Reviewing network/filtering/monitoring/incident logs, where possible
- Encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- Consulting stakeholders – including staff/parents/carers about the online safety provision
- Monitoring improvement actions identified through discussion, training and the use of the 360-degree safe self-review tool.

Reporting

- Record keeping of any incidents regarding online safety are recorded on CPOMS.
- The school will record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse.
- The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.
- We will ensure there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community are frequently made aware of the need to report online safety issues/incidents
- Reports will be dealt with as soon as is practically possible once they are received
- The Designated Safeguarding Lead, Computing coordinator and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include:

    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse.
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances or Cyber or hacking offences under the Computer Misuse Act

- Copyright theft or piracy

- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the record (CPOMS)
    - Once this has been completed and fully investigated the issue will need to be judged whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

        o internal response or discipline procedures
        o involvement by local authority
        o police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies and members of staff (DSL/Online Safety Lead) to support peers e.g. support for those reporting or affected by an online safety incident
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- Learning from the incident (or pattern of incidents) will be provided to:

    - The Online Safety Lead
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates

- local authority/external agencies, as relevant.

How will the risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. It is also key to highlight that the idea of "overblocking" is referenced at St Martin's in line with the suggestions made by UK Safer Internet Centre. This is to ensure that there are not "unreasonable" restrictions, which then hinder teaching and learning opportunities for children in regards of making choices and learning how to avoid potential risks growing independence and resilience. In relation to the idea of "overblocking" staff must be very aware of teaching points and potential issues that may arise ensuring they are providing teaching opportunities to guide and support pupils successfully. In terms of online safety neither the school nor Sandwell Council can accept liability for the material accessed, or any consequences resulting from internet use.

The school will audit (alongside our IT support partner) computing equipment used to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

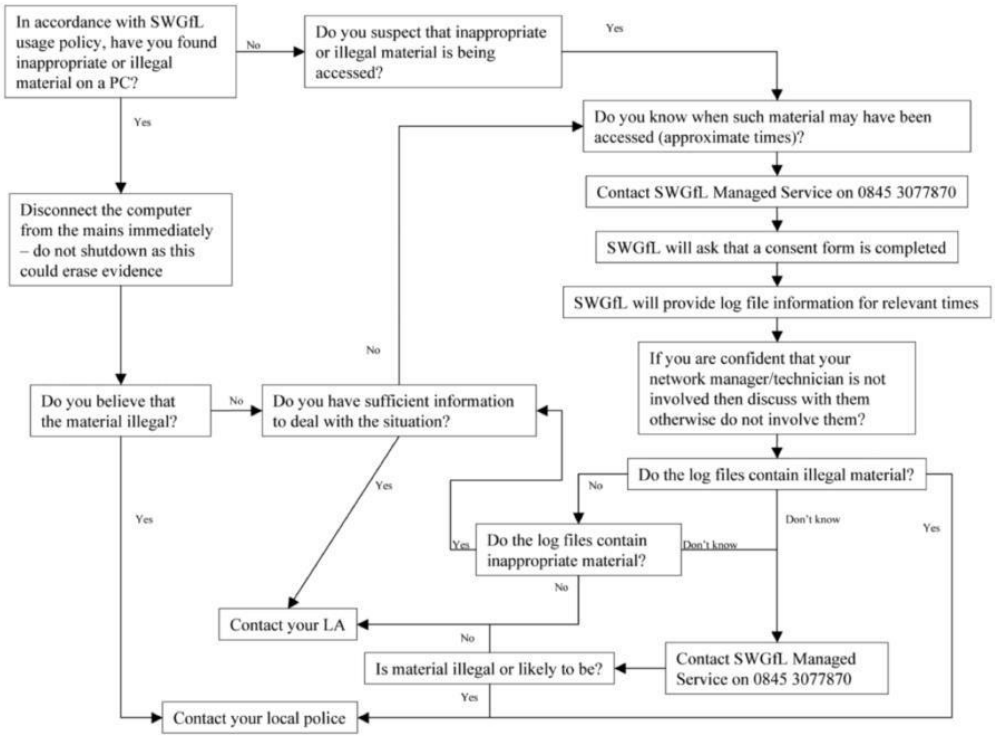
Methods to identify, assess and minimise risks will be reviewed regularly.

In the event of users not following guidelines, the following responses in the flow chart must be followed. This involves apparent or actual misuse appears to involve illegal activity.

For example: criminally racist material, inappropriate images of children, etc.

To identify these acts such as the Computer Misuse Act of 1990, Criminal Justice and Courts Act 2015, Communications Act of 2003, etc can be referenced.

The SWGfL chart identifies who should be notified and how to preserve evidence.



How should website content be managed?

The contact details on the school website should be the school address, e- mail and telephone number. Staff or pupils' personal information must not be published. The Headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission. Pupils' full names will not be used anywhere on the website or social media, particularly in association with photographs. Parental permission is obtained and recorded on SIMS. A copy of the consent is shared to staff annually, organised by office staff.

Social Networking

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations.
- Pupils will be advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address,

mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space.
- They should consider how public the information is and consider using private areas.
- Advice should be given regarding background detail in a photograph, which could identify the student or his/her location e.g. house number, street name or school.
- Teachers should be advised not to run social network spaces for student use on a personal basis.

Managing e-mail.

If using email:

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communications or in any way digitally or arrange to meet anyone without specific permission.
- Permission must be given by parents for children to receive their own e-mail address account and access to it.
- Emails from parents should be directed to the Office via our school website.

Office 365

If using Office 365:

- Children are taught how to use Office 365 effectively.
- Children should be a member of a select group based on their year and their access is limited.
- Permissions are limited, only having access to Outlook, their year group Sharepoint and specific applications to support learning and home learning e.g. Word and PowerPoint.
- Groups are checked regularly.
- Children understand if there are any issues regarding any online portal such as Office 365, or approved online accounts (Spelling Shed etc.), they are to report it to an adult immediately. This could be at school if they are situated there or at home.
- Any reports will be investigated and evidence collected to rectify any issues.
- Online Safety using Office 365 must be constantly reflected on and changes made if any issues arise.
- Teachers provided specific passwords for children that can be changed on request.

Mobile technologies

Mobile phones are not permitted in classrooms, which is evident in our Staff Code of Conduct and Acceptable Use Agreement. Staff personal mobile phones and tablets should

be kept in the staff room or a safe place (except for non-class based SLT).

Phones belonging to children should be handed into the office in the morning and collected at the end of the school day. The office is not responsible for the mobile phone, and it is the responsibility of the pupil to collect it within office time. Further information regarding this can be found in the mobile phone policy.

Data Protection

Personal data will be recorded, transferred, processed and made available according to the Data Protection Act 1998. This states personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Accurate
- Secure
- Kept no longer than necessary
- Transferred to others with adequate protection only
- Processed in accordance with the data subject's rights

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018.

It sits alongside the GDPR, and tailors how the GDPR applies in the UK.

There are 7 principles that apply:

1. Legality transparency and fairness
2. Purpose limitation
3. Minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

There are 8 rights of data subjects that need to be adhered to:

- **The right to be informed:** *Data subjects should be clear and what, why, and in what way, P11 will be processed.*
- **The right of access:** *Data subjects have the right to learn what PII is held on them, by whom and why.*
- **The right to rectification:** *Data subjects can request corrections to their PII*
- **The right to erasure:** *Data subjects can request to be forgotten*
- **The right to restrict processing:** *Data subjects can ask organisations to stop processing their PII.*
- **The right to data portability:** *Data subjects can ask for their PII in machine readable format or to have it sent to another organization.*
- **The right to object:** *Data subjects can object to organisations processing their PII.*
- **Rights in relation to automated decision making and profiling:** *Protection against targeted marketing and decision making.*

St Martin's C of E will ensure that:

- Personal data will be held no longer than necessary
- That data held is accurate, up to date and inaccuracies are corrected
- Personal data will be obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with "Conditions for Processing"
- There is a Data Protection Policy
- Responsible persons are identified and appointed
- It has clear storage, security and transfer for personal data
- The policy considers cloud storage/cloud computing
- Personal data is password protected
- Devices used are password protected
- Data is securely deleted from devices
- Devices will have malware and trusted virus checking software

Introducing the Online Safety policy to pupils

Online Safety rules will be posted around school where children use computers and other technology. Users will be informed that network and internet use will be monitored. Children will have regular Online Safety discussions and activities to promote its awareness in school, teaching children about the risks and benefits of technology and how it is and can be used. In addition to this, it allows staff to be aware of what children are accessing and what they are showing interests in digitally in and out of school. Staff then will report any trends during Online Safety discussion points in staff meetings, briefings, SLT or can go to the Safeguarding/online safety lead immediately if they have any concerns.

Children must also be made aware that Online Safety relates to several rules and laws. Data collected by ChildNet recently that suggests that children and young people are unaware of many of the rules, laws and consequences to do with online safety. Therefore, it is important that children are properly educated about these and potentials risks and consequences. In addition to this, we aim to foster confident digital citizens that know how to report effectively and independently as it has been suggested in the same data that some would not be confident in reporting acts such as online bullying.

As they progress through the school, children will be taught how to become a positive member of the digital world. These **SMART** tips (from Childnet International – www.childnet.com) will be shared with the children and visible for them to refer to whilst using technology in school (Appendix 2).

Safe – Keep safe by being careful not to give out personal information – such as your full name, e-mail address, phone number, home address, photos or school name – to people you are chatting with online.

Meeting – Meeting someone you have only been in touch with online can be dangerous. Only do so

with your parents' or carers' permission and even then, only when they can be present.

Accepting – Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable – Information you find on the Internet may not be true, or someone online may be lying about who they are.

Tell – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

Reporting should also be continually taught. Children will be taught about different ways to report and what to do in a variety of scenarios. They will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations:

CEOP – Report Abuse

NSPCC - https://learning.nspcc.org.uk/nspcc-helpline

Childline if they need to talk through concerns 0800 1111

How will complaints be handled?

Complaints of internet misuse will be dealt with by a senior member of staff; All children will be taught to use the Internet safely and the role of CEOP (Child Online and Exploitation Protection Centre) to monitor and report abuse; Any complaint about staff misuse must be referred to the Head teacher, unless it is the Head Teacher where complaints will be sent to Chair of Governors; Parents and pupils will need to work in partnership with staff to resolve issues.

Parents and Online Safety

At St Martin's, all input and opinions are valued. The school will always strive to deal with any issues face to face. Parents are advised to not post any issues about the school on any social networking sites. Furthermore, the school advises that parents avoid posting anything on social media sites that include pictures of children other than their own. This is always addressed at the start of any community/parent event.

St Martin's work hard to work as a community to safeguard and ensure children are safe. Children's ability to access technology, devices and use online facilities outside school is also very important however it is important that those who are looking after children outside school hours are also provided with opportunities to learn more about preventative measures, potential risks and be confident of where to go or who to contact in the event of any problems in relation to online safety. Therefore, as mentioned above, we provide a range of ways parents and guardians can stay up to date with information, ask questions if

needed, details of suitable technology, apps, current risks, etc.

One way we do this, is through workshops. Parents throughout school are provided with the opportunity to attend workshops linking to online safety. Links and additional information are available on our website, shared via our newsletter and through specific online safety letters (when appropriate). It is also important to mention that any issues relating to online safety, safeguarding and behaviour are logged on CPOMS. Steps are then put in place to support children and families further regarding this.

In working in close partnership with parents, guardians and the wider community to promote effective online safety for all. Views of the pupils and parents are used regularly to improve online safety at our school. In addition to this, information within hubs and from other sources if used to provide effective provision. Feedback is collected regarding online safety and helps to inform the need for specific further information, additional workshops, etc. Parents and guardians are also able to make requests regarding topics they would like further information about to ensure safeguarding of children is as effective possible. As suggested, a close relationship in and out of school regarding online safety helps for us to understand how children may be using technology frequently, how trends may be changing and how we can plan effectively to provide the best and most worthwhile learning opportunities for our children.

We encourage parents to regulate online access at home on all devices. This not only supports parents/guardians in being aware of when their children are using devices and accessing the internet, but it promotes a healthy “screen time and green time”, a period of using technology and being disconnected. We advise and provide parents and guardians with information regarding parental and technical control. POS (Parent Over Shoulder) is also encouraged. This is where children access technology and use online devices in a space that they can be monitored, for example a family room. We also advise parents on how to find out about new technology and software by spending time researching and using the technology with their child, so they are aware of any potential risks and if it is of a suitable content. Recent data shows that children are accessing technology for longer periods of time at all ages therefore we must also work together to ensure we are teaching children how to look after and prioritise their wellbeing and mental health in relation to using technology.

Remote Learning

For information regarding this, our remote learning policy and plan should be referenced.

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
PHSE/RSE Links	Being Me	Celebrating Differences	Dreams and Goals	Healthy Me	Relationships	Changing Me
Year 1	Self-Image and Identity Privacy and Security	Online Bullying	Managing Online Information Copyright and Ownership	Health, Well-being and Lifestyle	Online Relationships	Online Reputation
Year 2						
Year 3						
Year 4						
Year 5						
Year 6						

The ProjectEVOLVE toolkit is based on the UKCIS framework "Education for a Connected World" (EFACW). This framework covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from early years right through to eighteen. These outcomes or competencies are mapped to age and progress.

Appendix 2 – SMART rules (childnet.com)