ST.MARK'S CE SCHOOL

ONE SCHOOL - SERVING ALL - THROUGH EXCELLENCE

Online Safety and Digital Technology Policy

Policy Statement and Guidelines

Date: Summer 2026

Review: Summer 2027

E-safety and Internet use Policy

1. Introduction

The Internet is an essential element in 21st century life for education, business and social interaction and is a statutory part of the national curriculum as well as a necessary tool for staff and pupils. Throughout this policy

ICT will refer to all digital technology, media and platforms. Stakeholders refers to all students, staff, governors, volunteers and the wider school community.

The use of the Internet provides benefits including

· Improved subject learning across a wide range of curriculum areas.

· Improved motivation and attitudes to learning raising educational standards

· Development of independent learning and research skills.

· Prepares children for further exploration of ICT.

· Enhance the school's management, information and business administration systems. ·

Facilitates exchanges of curriculum and administration data with the LA and other

stakeholders.

· To celebrate student's work, and promote the school through a maintained school website and other facilities.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Support students in knowing and understanding that:
    - The Internet and digital communications are important
    - Internet use will enhance learning
    - It is important to evaluate Internet content and keep themselves safe.

3. Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and students;
- A comprehensive, agreed and implemented e-Safety and digital technology Policy;
- Secure, filtered and monitored broadband from Southampton County Council as well as use of other solutions including Securly;
- A school network that complies with the national standards, specifications and legislations.

4. Limiting E-Safety Risks

E-Safety is the process of limiting risks when using Information and Communication Technology (ICT). E-Safety is primarily a safeguarding issue not a technological issue which relates to the use of all ICT - fixed or mobile,
current, emerging and future ICT.

ICT is used daily as a tool to improve teaching, learning, communication and working practices to the benefit of our stakeholders and those that work to support them. The use of ICT is recognised as being of significant benefit to all members of our community, in personal, social, professional and educational contexts. However alongside these benefits are potential risks that we have a statutory duty of care to manage, to ensure they do not become

actual dangers to all our stakeholders.

At St Marks, the policy in place considers the following issues:

- the acceptable use of ICT by all users;
- e-safety procedures, e.g. incidents of misuse of ICT by users, safeguarding incidents when a user is at risk of or has come to actual harm through the use of ICT;
- e-safety training for staff, which is regular and robust and forms part of safeguarding training and e-safety training for pupils
- the technology available to users, its security features and settings, e.g. virus protection, filtering and monitoring;
- a named person with responsibility for e-safety, which should ideally be a member of the senior management team and is not necessarily the systems manager, is primarily about safeguarding and not the technology itself.
- For St Mark's the named person with overall responsibility for e–safety is Stephanie Bryant (Executive Headteacher)
    - Delegated responsibility for e-safety is Chris Lovett (Systems Manager).
    - Delegated responsibility for e-safety education is Conor Soffe - Computing Subject Leader (Primary) and Phil Bagge - Head of Computing (Secondary).

The term 'Staff' is used as a broad term within this policy and includes every adult who works on the school site as well as volunteers, governors and stakeholders.

St Mark's e-Safety and Policy must cover the safe use of ICT technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate all stakeholders about the benefits and risks of using technologies both in and away from school. It will also provide safeguards and rules to guide stakeholders in their online experiences.
St Mark's e-safety policy will operate in conjunction with other policies, procedures and processes in place at school including policies for Social Media, Pupil Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children plus the Home-School Agreement.

5. E-Safety Risks & Issues

E-Safety risks and issues can be roughly classified into the 4 C's:

· Content, Contact, Conduct and Commerce.

The following are basic examples of the types of e-safety risks and issues that could fall under each category, but is not an exhaustive list.

Content:

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information (including fake news)
- Exposure to socially unacceptable material such as that which relates to radicalisation, extremism, terrorism or those inciting violence, hate or intolerance, suicide, self-harm
- Exposure to illegal material, such as pornography
- Plagiarism

Contact:

- Subject to harmful online interaction with other users.
- Grooming using ICT, leading to sexual assault and/or child sexual exploitation
- Peer-to-peer pressure
- Bullies using ICT (email, mobile phones, chat rooms etc) as a way to torment their victims
- Commercial advertising

Conduct:

- Personal online behaviour that increases the likelihood of, or causes harm, such as making, sending or receiving explicit images
- Online forms of bullying, harassment or illegal behaviour

Commerce:

- Risks such as online gambling
- Inappropriate advertising
- Phishing and/or financial scams

6. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education (from Sept 2026)
- RSE and Health Education (Until 31 Aug 2026)
- Searching, screening and confiscation

It also refers to the DfE's guidance on safeguarding learners vulnerable to radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

6.1 Protecting Personal Data

Personal data will be processed and made available according to our data protection policy and Data Protection Legislation.

7. Roles and responsibilities

7.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and

monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems; •

Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning; •

Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

7.2 The Executive Headteacher

The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

7.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Systems Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Systems Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy •

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least

annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

7.4 The Systems Manager and IT Team

The Systems Manager and IT Team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy •

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

7.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking to the Executive Headteacher or one of the DSL deputies (another member of staff can show you who your nearest DSL is)
- Following the correct procedures by contacting the Systems Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

7.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet found in their registration packs on enrolment at the school, available as part of this policy and on our website.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

7.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

8. Infrastructure & Technology

Education IT advisors recommend that all organisations providing services to school stakeholders use an accredited service supplier to deliver filtered Internet access, configured to their own local circumstances and requirements.

Under the accreditation scheme, a product for filtering Internet content must meet or exceed the following requirements from the Department for Education, which can be found here: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard

St. Mark's CE School's firewall is provided by Hampshire County Council through Southampton City Council for devices connected to the school's network. Virus protection is purchased through a McAfee approved supplier. It is the school's responsibility to ensure that the virus definition files are updated regularly on all school machines to maintain protection, this is currently through McAfee Agent. Monitoring Systems – to keep track of who accessed what, when and on which computer - for pupils is currently supplied through Securly.

Filtering and content controls are provided by Southampton City Council ICT Strategy Team, using a company called TalkStraight and a service called Fortinet. This uses a nationally approved database of keywords and URLs which it filters. Additional keywords and URLs can be added to the filter by contacting ICT Strategy, telephone: 023 8083 4555. For more information contact the school office.

We additionally use Securly for students, which adds additional filtering and monitoring platforms and functionality. This system emails appropriate staff with details of e-safety incidents including accessed blocked content or worrying phases/words in content and keyword searches.

Managing Filtering

St Mark's Church of England School will work with Southampton City Council and appropriate partners to ensure systems to protect pupils are reviewed and improved. If staff or students come across unsuitable on-line materials, then the site must be reported to St. Mark's IT support team and DSL. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

9. Teaching and Learning

9.1 Why the Internet and ICT are important

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 Internet access and ICT as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for stakeholders.

9.2 Internet use will enhance learning

The school Internet access will be designed for all appropriate stakeholder's use and will include filtering appropriate to the age of users. Students will be supervised by a member of staff when using the Internet. Appropriate stakeholders will be taught what Internet use is acceptable and what is not and given clear

objectives for its use. Appropriate stakeholders will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will be shown how to publish and present information to a wider audience. Staff will ensure pre-selected websites for use are appropriate for the age of the users.

9.3 Appropriate stakeholders will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by appropriate stakeholders complies with copyright law. They will be taught the importance of cross-checking information before accepting its accuracy and validity. They will be taught how to report unpleasant Internet content correctly.

9.4 Taught Curriculum Content

The school ensures that pupils are taught a broad and balanced curriculum and covers the requirements of the National Curriculum to ensure that e-safety and digital technology are taught fully. Online safety and digital literacy teaching, including AI literacy, will be personalised to meet the needs of pupils with SEND and vulnerable children, ensuring accessibility, understanding, and relevance, in line with the *Equality Act 2010* and safeguarding duties.

Pupils will be taught about online safety and digital technology as part of the curriculum: **All** schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Internet derived materials by appropriate stakeholders complies with copyright law. They will be taught the importance of cross-checking information before accepting its accuracy and validity. They will be taught

Possible teaching and learning activities can be found at https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

10. Managing Internet Access

Information system security

School ICT systems security will be reviewed regularly. Sites deemed unsuitable for school use will be filtered and blocked accordingly. Appropriate stakeholders have the responsibility to inform Chris Lovett, the System's Manager and a member of SLT if they are concerned about Internet content seen in school. Virus protection will be updated regularly. Security strategies will be discussed internally and with relevant parties where necessary. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offense under the Computer Misuse Act 1990.

11. Internet Code of Conduct

- Students should be supervised at all times when using the Internet. Unsupervised pupil use of ICT resources

is not permitted at St Mark's. This could mean for older students that there is a member of staff (i.e. the Reading and Homework Champion) with them whilst using ICT equipment.

- Access to school systems must be with a unique login combination, which must not be made available to any other user.
- Access will be by a variety of methods including teacher demonstration, through links provided and suitable independent supervised research etc.
- All Internet activity should be appropriate to the user's professional activity or their education. ● Staff may use Internet facilities for non-business research or browsing during meal time breaks, or outside of work hours, provided that all other Internet usage policies are adhered to.
- Internet activity that threatens the integrity or security of the school's systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites or content such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related, extremist, terrorist, hate related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed and could face legal action, including being reported to the police or appropriate authority. ● The Internet must not be used to download entertainment software or games, or play non sanctioned games against other Internet users.
- Uploading materials or files to School or City Council systems must only be performed by authorised users on machines that have virus protection to the latest corporate standards and with appropriate authorisation from the relevant departments.
- Downloading of files to school systems using ftp, email and http must be carried out with an appropriate level of care and thought. Problems arising from the installation of files, utilities and software/updates obtained by such methods are the school's responsibility unless directed to do so by representatives of the City Council or their agents. Virus infection and subsequent removal caused by such methods on machines without protection to the latest corporate standards will be the school's responsibility. If carried out intentionally/maliciously the user(s) responsible could face disciplinary/legal action.
- The Internet must not be used to engage in any activity for personal gain or personal business transactions. ● The Internet must not be used to conduct or host any on-going non-school related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club/forum.
- The Internet must not be used for personal or commercial advertisements, solicitations or promotions, except where authorised to do so.
- The use of an ICT system without permission or for a purpose not agreed by the school could constitute a criminal offense under the Computer Misuse Act 1990 and may result in legal action. ● To ensure compliance with acceptable use of ICT the school reserves the right to monitor and record activity in appropriate areas. All users should therefore have no expectation of privacy in respect of their Internet activities when using the school's ICT facilities/resources.

11. 1 Email Code of Conduct

- Access to email should only be via the authorised user name and password, which must not be made available to any other user.
- Students may only use approved email accounts on the school system and must be supervised. ● Pupils must immediately tell a teacher if they receive offensive or inappropriate email/material or email/materials that upsets them.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Other users must be cautious and consider GDPR and related policies. ● Normally, access to another staff user's email account will not be granted to anyone. However, there are occasions when such access may be legitimately needed, e.g. to aid investigation of suspected irregularities; upon summary dismissal of an employee; during suspension or prolonged absence of an employee; where the retrieval of information is necessary to allow continuation of work in hand by the user whose ID/password combination is to be circumvented.
- Links/attachments from unknown sources should not be opened, but deleted immediately.

All attachments should be scanned for viruses.

● Users are responsible for all email sent and for contacts made that may result in email being received. ● Posting anonymous messages and creating or forwarding chain letters is forbidden. ● As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

- Emails sent on school business to an external organisation should be written carefully, and authorised if appropriate, in the same way as a letter written on school headed paper.
- Messages that contain abusive or objectionable language, that libel others, that infringe the privacy rights of others, could be classed as criminal or for whatever reason are forbidden.
- Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non education related activities, except where authorised to do so.
- Personal or otherwise sensitive data must not be transferred via email unless the security of the data whilst in transit can be assured and GDPR policies must be adhered to at all times. It is always recommended to find more secure methods of transfer (i.e. AnyComms, NHS Secure etc)
- Standard email addresses in Southampton follow the format of *initialsurname@school*. Care will be taken when considering the format of individual pupil email addresses, as the recipient would be aware of the sender's full name using this format and so for students we have (from September 2023) chosen to use *initalsurnameyearofadmission@* for pupils.

11. 2 Cyber-bullying (To be read in conjunction with our Social Media, Behaviour and Safeguarding Policies)

11.2.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

11.2.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their classes/tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so. The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Stakeholders will be advised never to give out

-

12. Social Networks, Chat Rooms, Instant and Text Messaging Code of Conduct (Read in conjunction with Social Media Usage policy)

Staff must use only school-provided or authorised email accounts and AI communication tools for school business and communication with pupils or parents, maintaining professional boundaries and data security in line with safeguarding and data protection policies.

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Stakeholders will be advised never to give out personal details of any kind which may identify them or their location (including that of others). Ideally students would use only moderated social networking sites, e.g. G Suite Platforms. Stakeholders will be advised that the use of social network spaces outside school brings a range of dangers for those that use it. Stakeholders will be advised to use nicknames and avatars, where appropriate (i.e. for pupils), when using age appropriate social networking sites.

● Students should only be given access to secure, age appropriate chat rooms and social networks, which are moderated by a member of staff, or recognisable, identifiable and approved adult. ● The use of such websites should only be permitted within an educational or professional context. ● The school Facebook, Twitter, YouTube and Instagram accounts are monitored and administered by appropriate staff, with the Executive Headteacher having oversight. (Also read Social Media Policy) ● Staff should familiarise themselves with any chat room being used, to ensure that it offers a genuine educational experience when used in school.

● Students should be supervised at all times when using such websites.

● Students should be taught to understand the importance of personal safety on the Internet, i.e. taught never to give out personal information or to arrange to meet someone they have met online. ● Access to Internet related services such as instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to a device which provides online access. For this reason, we need to ensure that pupils are taught safe and responsible behaviours whenever using ICT.

● All stakeholders should be aware of St Mark's guidelines for the use of social networking sites. The guidelines are in place to protect stakeholders from allegations of misconduct/misuse in their use of networking sites at all times. (**See Social Media Policy**)

13. Published content and the School Website Code of Conduct (Read in conjunction with Social Media Usage policy)

A school website is maintained by the Executive Headteacher's PA and IT Team and celebrates students' work and promotes the school, its information as well as providing all statutory information. Stakeholder personal contact information will not generally be published. The contact details given online will be the school office. The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

● The school website will be accessed via a home page using the domain name www.stmarksschool.co.uk ● The production and publication of any unofficial websites is strictly forbidden and, if undertaken, will be actively pursued by the City Council for removal on behalf of the school.

● Only the designated staff member(s) within the school may upload material to the school website and all material for the website must be monitored and approved by the person(s) responsible. ● All usernames and passwords to access the administration site must not be given to any other stakeholders. If other people know this information, the Systems Manager and Executive Headteacher should be alerted immediately, the password changed and the means of which they have found this information investigated and action taken as necessary.

● Images of stakeholders should be classed as personal data under the terms of Data Protection. Therefore, using such images for school publicity purposes, i.e. school website, will require the consent of either the individual concerned or in the case of pupils, their legal guardians. This can be using forms completed at registration.

- Full names and personal data of all stakeholders must not be published on the school website without consent. Where possible the school details will be given as the main point of contact.

14. Publishing Student's Images and Work Code of Conduct (Read in conjunction with Social Media Usage policy)

- Photographs that include stakeholders will be selected carefully so that individuals cannot be identified or their image misused, unless consent is given. We consider using group photographs rather than full-face photos of individuals.
- Stakeholder's full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs, unless consent is given.
- Written consent from parents or carers will be obtained before photographs of pupils are published on the school website including use of forms completed on registration and via SCOPay Trips and Events. ● Work can only be published with the consent of the pupil and parents/carers except for educational purposes as per data protection. Consent will be sought from parents at admission to the school. ● Pupil image file names will not refer to the pupil by name.
- Parents will be clearly informed of the school policy on image taking and publishing (see Social Media and Safeguarding policies).

15. Managing Videoconferencing & Webcam Use (Also read in conjunction with video call agreement consent)

- Video conferencing should use the educational broadband network (where practically possible) to ensure quality of service and security. This may vary if stakeholders are engaging from home.
- Pupils must ask permission from the supervising teacher before making or answering a video conference call. Parents must sign an agreement before this takes place, which is now at registration. ● Videoconferencing and webcam use will be appropriately supervised for the students' age following guidance and etiquette in the signed agreement.

16. Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and an appropriate assessment will be carried out before use in school is allowed. Stakeholders should note that technologies such as mobile phones/tablets with Internet access can bypass school filtering systems and present a new route to undesirable material and communications as such these are currently deemed as inappropriate for use by pupils, visitors, guests to connect to our network.

17. Mobile Devices – Clarify Use, Sanctions, and AI Device Controls

Mobile devices have now become an everyday technology with most stakeholders owning or having use of at least one type of these devices. They have become an essential part of our lives. However, they still have associated dangers and require consideration in terms of e-safety. At St. Mark's…

- Mobile devices will not be used during lessons or formal school time, unless it is a school device, in which case it will be used appropriately and for legitimate reasons. The sending of abusive or inappropriate content is forbidden. Please refer to Mobile Phone Policy and Staff Code of Conduct at St Marks.
- The use of cameras in mobile devices is not permitted whilst on the school site. No digital content should be taken of stakeholders without consent. The school will investigate any reported cases of such actions and this could lead to further action being taken.
- Games consoles/devices such as the Playstation or Xbox etc have Internet access which may not include filtering or can bypass our filtering and blocking systems. Care is required in any use in school or other officially sanctioned location/events. The school games consoles/devices will not be used to connect to players in other locations over the Internet and will only be used to play against actual players in front of the console unless consent is given by parents or sanctioned by appropriate staff.
- At no time should staff use their personal mobile phone to communicate with/or send data to a pupil or the parent of a pupil, except when utilising specific softphone applications that allow for use via school systems.

● A mobile phone may be issued to a member of staff so that contact may be made by the Executive Headteacher either when the school main phone is in use or in an emergency out-of-hours context. This can be extended to the use of specific applications on personal phones that utilise the school telephony systems.

● A strict no use of mobile phones by students on the school site is in place at St. Mark's and breach of this rule will incur sanctions.

- Mobile devices, including AI-enabled devices (phones, tablets), are prohibited during lessons and formal school time unless explicitly authorised for educational use on school devices. Personal devices must be handed in securely on arrival. Use of AI applications on personal devices is restricted to prevent exposure to inappropriate content or data breaches. Breaches will result in sanctions consistent with the Behaviour Policy, including confiscation and parental notification.
- This clarification supports safeguarding and compliance with *Education Act 2011* and emerging AI device management best practises.

18. Policy Decisions

18.1 Authorising Internet Access

● All staff must read and sign to agree to the 'Stakeholder Code of Conduct for ICT' (**see Appendix B**) before using any school ICT resource, this includes all appropriate stakeholders i.e. volunteers, governors and visitors.

● All staff must read and confirm they agree to abide by the Social Media, Acceptable Use of Internet and all other associated policies that form part of staff non-negotiables.

● Parents and pupils will be asked to sign and return consent form(s) as needed.

19. School Password Security

A safe and secure username / password system is essential to maintain security and prevent any breaches. It will apply to all school systems where this is necessary and required, including networks, devices, Google and educational/administrative platforms or software etc.

School Password Security Statements

• All users will have clearly defined access rights to school technical systems and devices. • All school networks and systems will be protected by secure passwords that are regularly changed. • The "administrator" passwords for the school systems, used by the technical staff must also be available to the Executive Headteacher or other nominated senior leader and kept in a secure place. Consideration should also be given to using two factor authentications for such accounts.

• All users (adults and students) will have responsibility for the security of their username and password 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.

• Windows passwords for new users and replacement passwords for existing users will be allocated by the IT Team.

• Google and other platform passwords for new users and replacement passwords for existing users will be issued through an automated process via e-mail or created and given directly to the person concerned (or via their class teacher/tutor where appropriate), initiated by the IT Team.

• Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below

Staff Passwords

• All staff users will be provided with Windows and Google username and passwords as described above. • Ideally staff passwords should be a minimum of 8 characters long and must include – uppercase character, lowercase character, number and special characters. However, some systems have alternative password policies, but this is what is advised for all passwords.

• Ideally passwords should not include proper names or any other personal information about the user that

might be known by others

- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption). • Ideally Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school. • Should be changed as requested when logging in.
- Passwords should not be on display on desks or on noticeboards and should be kept secure.

Pupil Passwords

- All Primary students will be provided with a username and password by the IT Team, who will keep an up to date record of users and their usernames and passwords where appropriate.
- Secondary students will be provided with a username and an initial password by the IT Team and forced to change this on first login. The IT Team will keep an up to date record of users and their usernames with initial password.
- Users will be required to change their password regularly.
- Pupils will be taught the importance of password security.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability and skill of the children.
- Some platforms will use a generic class or school username and password which will enable them to access the platform.

20. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems, equipment or internet, we will follow the procedures set out in our policies (i.e. Behaviour Policy). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police or other such appropriate authority.

21. Examining electronic devices

The Executive Headteacher, and any member of staff authorised to do so by them (as set out in our behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or • Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will then follow agreed procedures and should consider:

- Making an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Executive Headteacher / DSL / appropriate staff member.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and/or Executive Headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or •
The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy and/or searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

22. Staff using work devices outside school

All staff members will take appropriate steps as detailed in the loan of equipment agreement form they complete when they are issued the equipment (unless this was issued due to role in the school in which case staff will follow the below guidance) to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) • Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable

use. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Systems Manager, or in his absence the IT Team.

23. Communications

23.1 Introducing the e-safety policy to students

All students and parents must read and sign the 'St Mark's e-safety and digital technology agreement' before using any school ICT resource.

- St. Mark's IT Charter will be posted in all rooms where computers are used and discussed with pupils regularly it also forms the background of all primary students once logged in.
- All stakeholders should be aware that network and Internet use will be monitored and any inappropriate activity followed up.
- e-Safety training will be embedded within the Computing curriculum, including the schemes of work or the Personal Social and Health Education (PSHE) curriculum.

23.2 Staff and the e-Safety policy

- All stakeholders will have access to the e-Safety Policy and its importance explained.
- Stakeholders should note that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Stakeholders will always use an appropriate search engine when accessing the web with pupils or when searching themselves.
- All appropriate stakeholders must read and sign the 'St Mark's e-safety and digital technology agreement' before using any school ICT resource.

23.3 Enlisting parents' and carers' support and educating them about online safety

- Parents' and carers' attention will be drawn to this policy in newsletters, consent forms and on the school website.
- The school will maintain a list of e-safety resources for stakeholders.
- The school will ask all new families to sign the 'St Mark's e-safety and digital technology agreement' when they register their child with the school.

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings where appropriate.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher (info@st-marks-southampton.org.uk) or a DSL (DSL@st-marks-southampton.org.uk) should the Executive Headteacher be unavailable.

Concerns or queries about this policy can be raised with any member of staff or the Executive Headteacher.

24. Training

All staff will receive comprehensive induction and annual refresher training on e-safety, including online radicalisation (Prevent Duty), grooming, data protection (UK GDPR), filtering and monitoring systems, and responsible AI use. Training will be role-specific, include AI ethics and risk mitigation, and be evaluated for impact.

This ensures alignment with KCSIE, Prevent, and emerging AI safeguarding requirements.

-

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such

content • Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element Training will also help staff:

• Develop better awareness to assist in spotting the signs and symptoms of online abuse • Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks • Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

25. Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety when used by those in the community, however currently that functionality is not possible for use by anyone that is not using a school sanctioned device.

26. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material through processes and systems described in the Infrastructure & Technology section of this policy. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor associated partners can accept liability for any material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. In addition the school carries out an e-safety assessment using the 360 safe tool. Risk assessments will explicitly consider remote learning environments, home ICT use, and the deployment of AI technologies to ensure safeguarding, data protection, and ethical compliance beyond the school premises, following DfE guidance on remote education and AI governance."

27. Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff in conjunction with the Systems Manager. Any complaint about staff misuse must be referred to the Executive Headteacher, who may then consult LADO or HR. Complaints of a child protection nature must be dealt with in accordance with St Mark's child protection procedures and policies. The complaints procedure can be viewed through the school's complaints policy which is available on the school website. Stakeholders will be informed of consequences for misusing the Internet if an incident occurs.

28. Writing, reviewing and monitoring the e-safety and digital technology policy

This policy relates to other policies including those for Social Media, Data Protection Policy & Procedures, Behaviour and Child Protection. The Executive Headteacher will liaise with the Systems Manager and Computing Subject Leaders. E-Safety and digital technology form part of the role of the Systems Manager.

All appropriate stakeholders share delegated responsibilities to ensure e-safety and digital technology needs of children and other stakeholders at St Marks. The Designated Child Protection Lead works in conjunction

with the Systems Manager to ensure e-safety and digital technology is a high priority.

The DSL or delegated member of staff logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Systems Manager in conjunction with other appropriate staff. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Our e-Safety Policy has been written by the school, external partners and government guidance. It has been agreed by senior management and approved by governors.

29. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy
- Privacy notices
- Complaints procedure
- ICT and internet acceptable use
- Social Media and Networking Policy

30. Useful Resources

Care for the family
https://www.careforthefamily.org.uk/

National Cyber Security Alliance
www.staysafeonline.org

CEOP
www.ceop.police.uk

Internet Matters
www.Internetmatters.org

NSPCC
www.nspcc.org.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parent Zone
https://parentzone.org.uk/

Digizen
http://www.digizen.org/

Childnet International
https://www.childnet.com/

Hampshire Police – e-Safety
https://www.hampshire.police.uk/advice/advice-and-information/online-safety/online-safety/

Appendix A- Mobile Phone – Acceptable use at St Mark's Church of England Primary School

St Mark's Church of England School
Parent and Student Mobile Phone Agreement

Your Child's name: _____

Class: _____

Your name: _____ (parent/carer) Please explain

why your child needs to have a mobile phone on them when they arrive/ leave school.

_____

_____

_____

Mobile phone terms of agreement

- Conditions set out in the 'e-safety and digital technology policy' mobile devices section must be adhered to. This policy is available on our website.
- Parents will need to briefly explain why their child needs to have their mobile phone on them in the space provided above.
- The phone is to be used for appropriate use only on the journey to or from school. · The phone must not be used by the child on school premises.
- Phones must be handed in to the teacher as soon as the child arrives at in class to be kept in the class safe or appropriately secure place.
- The phone must be clearly labelled with the student's name and class.
- The student is responsible for collecting the phone. Any phones not collected will be kept locked away until collection.
- Parents take full responsibility for the phone and their child's use of the phone during the journey to and from school.
- The school will take no responsibility for the loss or damage of any phone. ● Parents will be contacted if a child does not follow the agreement and the procedures noted in our behaviour policy with regards to mobile phones will be followed as necessary. ● Our policy is still that no mobile phones should be taken on residential/day trips organised by the school in school time.

By signing this consent form, we understand and agree with all the terms above and that failure to keep any part of the agreement may result in a complete mobile phone ban. I have discussed the mobile phone agreement with my child and will support the school in implementing it. This information will be held securely whilst your child attends St. Mark's as proof of consent/agreement and will not be shared (except where legally obliged to do so) or affect your rights under data protection legislation. If you wish to discuss this, please contact the school on 02380 772968.

Signed by parent_____ Date_____

I agree to follow the mobile phone agreement and have discussed how I will use my mobile phone with my parent/carer.

Signed by pupil _____ Date_____

Stakeholder Code of Conduct for ICT. (Appendix B)

Stakeholder Code of Conduct for ICT

(ICT will refer to all digital technology, media and platforms. Stakeholders refers to all pupils, staff, governors, volunteers and the wider school community.)

To ensure that all stakeholders, including volunteers and governors, are fully aware of their responsibilities when using any school ICT system or device, they are asked to sign this code of conduct. Stakeholders should consult the appropriate policy and procedures for staff. This would be the school's e-safety policy, code of conduct for staff and other staff handbooks including social media for further information and clarification.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner, this includes but is not limited to, any illegal purpose for example the transmission of any illegal content.

I understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

I understand that school ICT systems may not be used for private purposes without specific permission from the Executive Headteacher.

I understand that my use of school ICT systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect ICT security and I will not disclose any password or security data to anyone other than an authorised system manager.

I will not install any app/software/hardware or make any setting/security changes without permission. I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely as per data protection policy and procedures.

I will respect all associated legislation related to ICT such as copyright and intellectual property rights/legislation. I will report any incidents of concern regarding e-safety safety to the Systems Manager, the Designated Safeguarding Lead or Executive Headteacher.

I will ensure that electronic communications with all stakeholders including email, instant message and social networking are compatible with my role and that messages cannot be misunderstood or misinterpreted. (See social media policy)

I will promote e-safety with all students and stakeholders and will help them to develop a responsible attitude to ICT.

The school may exercise its right, at any time, to monitor the use of the school's ICT systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's ICT system may be taking place, or the system may be being used for criminal purposes i.e. storing unauthorised or unlawful digital media.

I have read, understood and confirm to abide by the Staff Code of Conduct for digital technology. Signed: _____ Date: _____

Name in Capitals: _____

Accepted for school: St Mark's CE School

This will be held securely in stakeholder files to comply with our legal duties and to show your agreement and consent to abide by the above and does not affect your rights or responsibility under data protection legislation. It will not be shared (except where legally duty bound). If you wish to discuss this please contact Stephanie Bryant, Executive Headteacher.

Rules for Responsible Internet Use

(Appendix C)

Responsible Internet Use at St Marks C of E School

The ICT systems are owned by the school. This Responsible Internet Use statement helps to protect students, staff and all stakeholders including the school by clearly saying what use of the computer resources is acceptable and what is not.

Irresponsible use may result in the loss of Internet access and could lead to disciplinary proceedings for stakeholders.

Network access must be made via the user's authorised account and password, which must not be given to any other person. Use of external storage devices is not allowed.

School computer and Internet use must be appropriate and responsible to the student's education or to other stakeholder activity and only with permission.

Copyright and intellectual property rights must be respected.

E-mails should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

Users are responsible for email they send and for contacts made.

Anonymous messages and chain letters are not permitted.

The use of unauthorised chat rooms is not allowed.

I will not give out any personal data and will report anything that I find upsetting to Mr Lovett, Systems Manager.

The school ICT systems may not be used for private purposes, unless the Executive Headteacher has given permission for that use.

Use for personal financial gain, gambling, political purposes or advertising is not permitted.

ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be
taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

(Appendix D) - St Marks C of E School e-Safety and Digital Technology Agreement

All pupils use ICT systems including Internet access as an essential part of learning, as required by the National Curriculum and to prepare them for their future lives. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and that they agree to abide by them and also to obtain parental consent to meet our legal duties.

Pupil:	***Class:***

Pupil's Agreement

O I have read understand and will follow the St Mark's Responsible Internet

Use. O I will use ICT in a responsible, safe and respectful way at all times.

O I know that all ICT use may be monitored and that irresponsible use may result in the loss of digital technology access.

Signed: Date:

Parent's Consent for Web Publication of Work

I agree that my son/daughter's work may be electronically published with/without a first name subject to the school policies on such publication.

Parent's Consent for Digital Technology use and access

I have read and understood the school ICT rules. I understand that the school will take all reasonable precautions to ensure that pupils are safe and cannot access inappropriate materials but I understand that this is not 100% secure due to the nature of ICT.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet or via some ICT.

Signed: Date:

Please print name:

Please complete, sign and return to the school office

This consent will be held securely on the child's file whilst attending St Mark's to meet our legal duties. This information will not be shared except where required by law. This does not affect your rights under data protection legislation. Please see our website for further details and contacts regarding your rights (www.stmarksschool.co.uk).