Digital Safety Policy

Introduction

The school Digital Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.
The purpose of this policy is to:

- establish rules for using the Internet and school electronic equipment.
- describe how these fit into the wider context of our behaviour for learning and PSHE policies.
- demonstrate the methods used to protect the children from unsuitable material.

The benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and carers. At St Mark's CE Primary School, we feel that the most effective ways of ensuring responsible Internet use by our children involves a combination of up-to-date education, site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Why the Digital Resources and Emergent Technology Are Important

The purpose of Digital Resources use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
Digital Resource use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. They are an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality access as part of their learning experience.

How Digital Resources Benefit Education

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to digital learning, national developments, educational materials and best curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and Government agencies.
- improved communications between the home and school.

How the Internet Will Enhance Teaching and Learning

Internet access at school is designed for pupil use and will include filtering of website content appropriate to the age of pupils. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access is planned to enrich and extend learning activities. 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 and retrieval.

Safety Across the Curriculum

It is vital that pupils are taught how to take a responsible approach to their own online safety. There are three main areas of risk.

Areas of risk	*Examples of risk*
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	• Advertising e.g. SPAM • Privacy of information (data protection) • Identity fraud (scams, phishing) • Invasive software e.g. Virus, Trojans, Spyware • Premium Rate services • Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	• Illegal materials • Inaccurate/biased materials • Inappropriate materials • Copyright and plagiarism • User-generated content e.g. You Tube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyber bullying • Contact Inappropriate (emails/instant messaging/blogging) • Encouraging inappropriate contact • Social Media

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through the SMART rules. These rules are displayed clearly in all learning environments and are embedded in all teaching and learning where technology is being used.

Education will be provided in the following ways:
- A subscription to the National Online Safety Primary School Scheme of Work programme will be provided as part of ICT/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school.
- Key messages will be reinforced as part of assemblies and tutorial/pastoral activities.
- Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Annual National Internet Safety Day provides a focus on a worldwide scale.

Education & Training – Staff

It is essential that all staff receive training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
• All new staff will receive training as part of their induction programme, ensuring that they fully understand the school policy and Acceptable Use Policies.

The Role of the Leader

The leader is the point of contact for issues and incidents, however certain responsibilities may need to be delegated to other staff e.g. Designated Senior Person/Child Protection Officer as appropriate.

Our leader is Mrs Adele Martinez
Our Governor is Mr **Gary Fairbrother** (Chair of Governors)

The role of the leader includes:

- Operational responsibility for ensuring the development, maintenance and review of the School's Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an incident occur.
- Ensuring the Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging advice/training for staff, parents/carers and governors.
- Ensuring the Head teacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person/Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

Security and Data Management

In line with the requirements of the General Data Protection Regulation 2018 (GDPR), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary

All staff are aware of the need to ensure that personal data (including data held on MIS systems) is kept secure at all times, and is used appropriately, whether in school, taken off the school premises or accessed remotely. If it is necessary for a member of staff to save personal data onto their home information system, they will consult with the Head teacher or Computing Subject Lead. See *Appendices for Technology and Internet Acceptable Use Agreements*.

Websites and Other Online Publications

This may include for example, pod casts, videos and blogs.
The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs of children will be used on the web site. Pupils' full names will not be used anywhere on the website.

Digital Media

All images of children or staff must be taken on the school cameras only, unless specific permission is given. These images must be downloaded onto the Teachers' area of the server, and will be deleted when necessary.

At St Mark's CE Primary School, we are aware of the issues surrounding the use of digital media online. At times, information such as text, photographs may be 'downloaded' from the internet for use in pupils' presentations. As part of our training staff and pupils will be made aware of the copyright laws. Text and images will be checked and monitored by staff.

As photographs and video of pupils and staff are regarded as personal data in terms of the GDPR Act 2018 school must have written permission for their use from the individual and/or their parents or carers. See *Appendix 3.*

Digital Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks and disadvantages:

	Staff and Other Adults				Pupils		
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	x				x		
Access to internet	x					X	
Use of mobile phones in lessons				X			X
Use of mobile phones in social time	X						X
Taking photos on mobile phones or cameras		X With permission from Head teacher			X On school ipads or cameras only		
Use of other mobile devices e.g. tablets, gaming devices	X				X On School iPads		
Use of personal email addresses in school, or on school network		x					X
Use of school email for personal emails		X					X
Use of messaging apps		X					X
Use of social media		X					X
Use of blogs		X					X

The school will provide access to the telephone, email and the internet for all staff for work related purposes. Staff are permitted occasional personal use of the telephone, email and the internet, outside their timetabled working hours. The school will not make a charge for this, provided the privilege is not abused. All digital communications should be professional in tone and content.

<u>**Mobile telephone**</u>:

Generally, staff's personal mobile phones should not be used in the school setting except for emergencies; they will remain locked away in a safe area during the school day. The use of a mobile

phone must not detract from the quality of supervision and care of the children.
However, staff may use their personal mobile phones as a means of contact during school trips and out of school activities.

Children are allowed to bring mobile telephones to school for emergency contact use only. These must be given to their class teacher or taken to the office for safe keeping. Children will not be allowed to use a mobile phone for any other purpose e.g. taking photographs.

Email

In our school the following statements reflect our practice in the use of email.

- All users are aware that email is covered by GDPR Act 2018 and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- We include a standard disclaimer at the bottom of all outgoing emails

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Instagram and online games forums etc. These sites provide users with simple tools to create a profile page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old.

These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

All staff must be aware of the following points:

- That they familiarise themselves with the sites 'privacy settings' in order to ensure the information is not automatic.
- That they do not conduct or portray themselves in a manner which may: -
  - ✓ Bring the school into disrepute
  - ✓ Lead to valid parental complaints
  - ✓ Be deemed derogatory towards the school and or/employees
  - ✓ Be deemed derogatory towards pupils and/or parents and carers

- ✓ Bring into question their appropriateness to work with children and young people
- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set as private.
- Pupils must not be added as 'friends' on any Social Network site.

Cyberbullying

Cyberbullying is the use of digital communication as a form of continued bullying. At St Mark's no type of bullying is acceptable. The school will provide key safety advice for the children, staff and parent about Cyberbullying.
See Government Advice
Cyberbullying: Advice for Headteachers and School Staff
Advice for Parents and Carers on Cyberbullying
Any incidents will be dealt with in line with the School's Anti-Bullying policy

Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. You may wish to consider this agreement as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff. See *Appendices*

1. Staff, Supply Teachers, External Staff, Visitor and Governor Digital Safety Acceptable Use Agreement *(Appendix 1a)*
2. Parent/Carer Digital Safety Acceptable Use Agreement *(Appendix 1b)*
3. EYFS Pupil, Parent/Carer Digital Safety Acceptable Use Agreement *(Appendix 1c)*
4. KS1 Pupil, Parent/Carer Digital Safety Acceptable Use Agreement *(Appendix 1d)*
5. KS2 Pupil, Parent/Carer Digital Safety Acceptable Use Agreement *(Appendix 1e)*

Dealing with Incidents

An incident log will be completed to record and monitor offences. This will be audited on a regular basis by the Digital Safety Lead or Head Teacher. See *Appendix 2.*

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP and Internet Watch Foundation (IWF).

Please note: **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.**

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

Inappropriate use

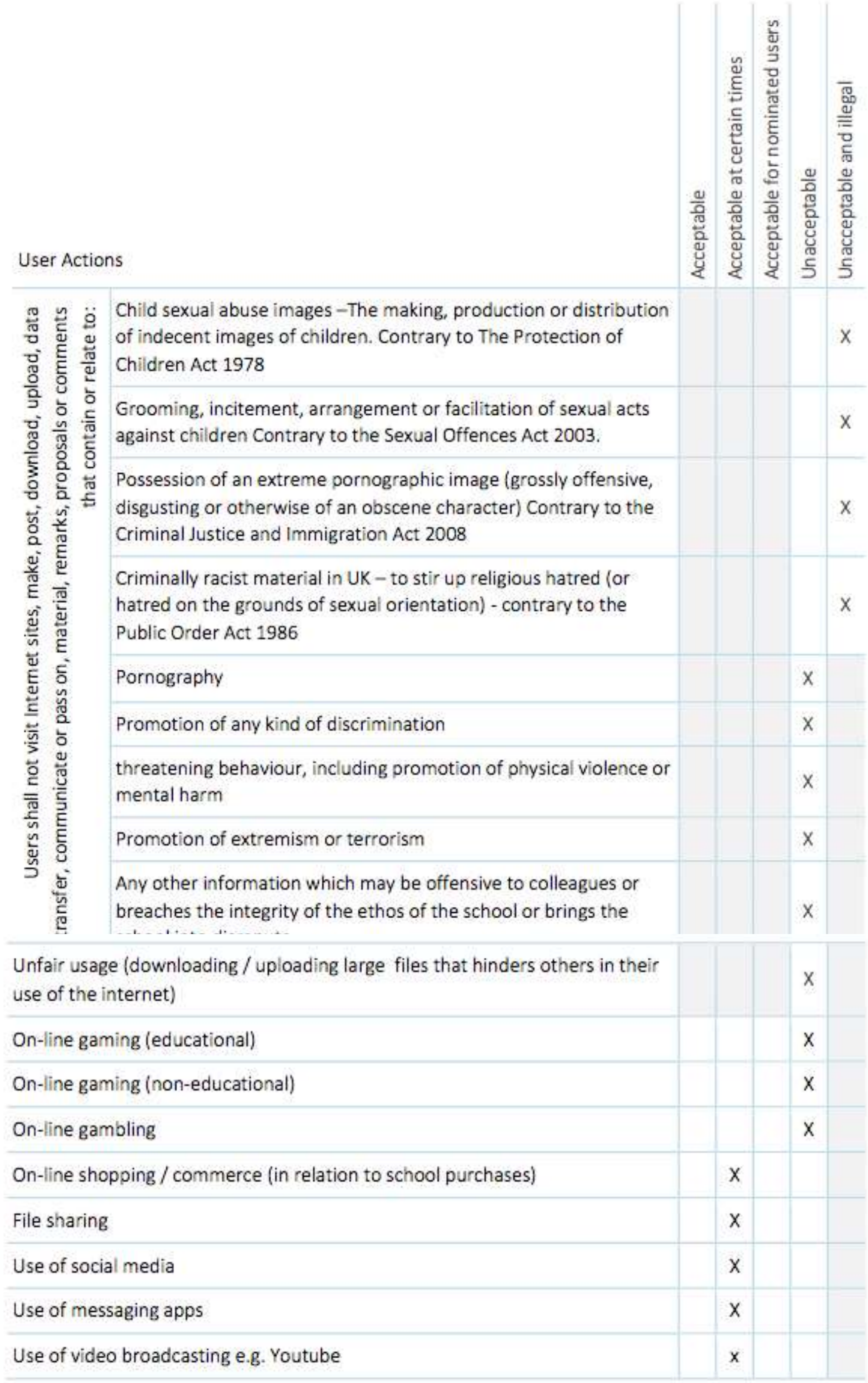
It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Incident	procedure and sanctions
Accidental access to inappropriate materials.	• Minimise the webpage or turn the monitor off • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent, 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform lead. • Enter the details in the Incident Log. • Additional awareness raising of issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

Dealing With Unsuitable or Inappropriate Activities

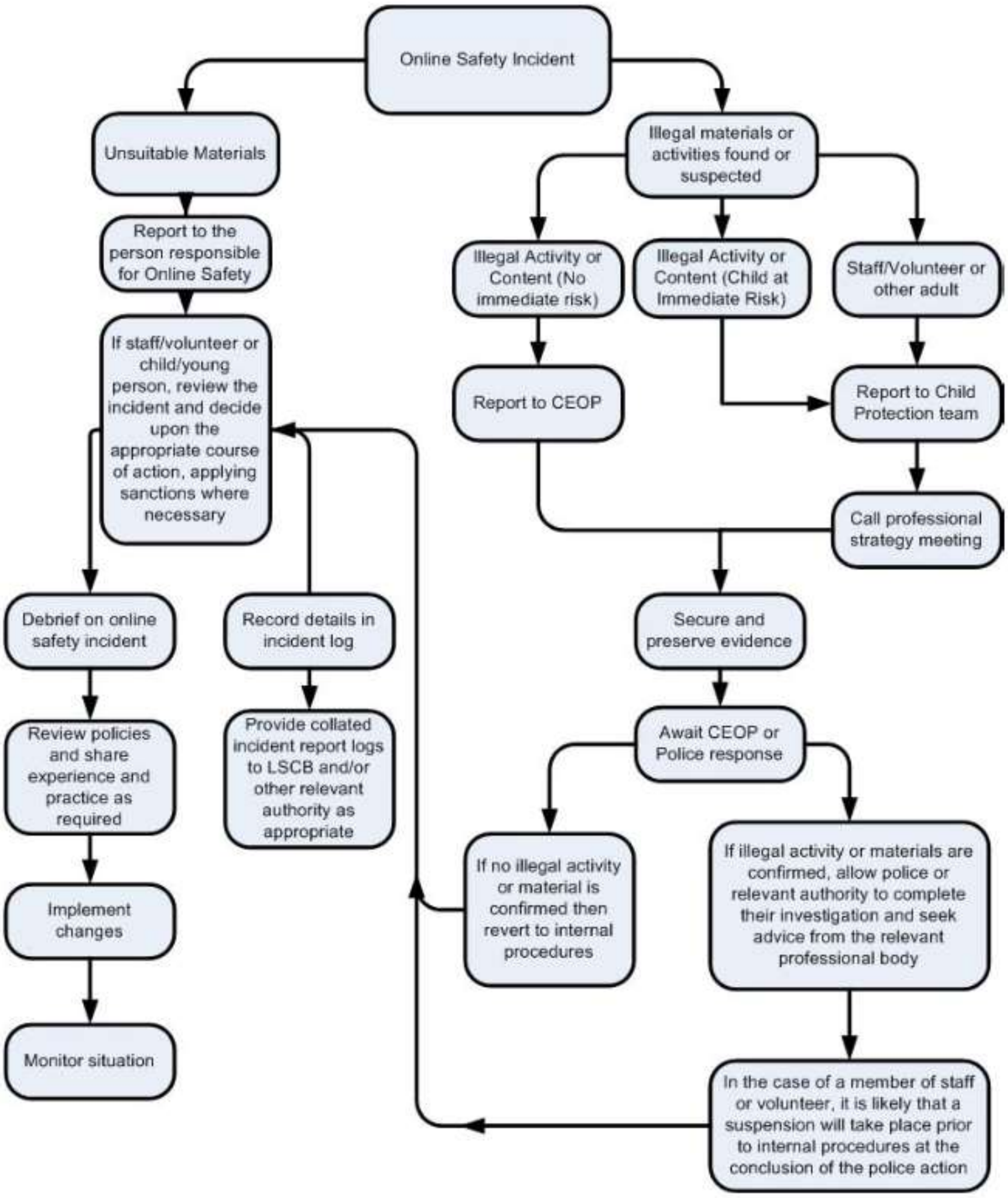
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school policy restricts usage as follows:



User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data ransfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce (in relation to school purchases)			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. Youtube			x			

If there is any suspicion that the web site or sites concerned may contain child abuse images, or if there is any other suspected illegal activity, see the Flowchart for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

<u>Infrastructure and Technology</u>

<u>Filtering and Virus Protection</u>

St Mark's School will ensure that the infrastructure/network is as safe and secure as possible. We subscribe to the Lancashire Grid for Learning/BT Connect and internet content filtering is provided by default. It is installed on all computers in school and configured to receive regular updates. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.

Staff are aware of the procedures for blocking and unblocking specific website.

Pupil Access

The children will only use the internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards the computer screen. Every possible precaution will be made by staff to ensure appropriate use of the internet by children

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through the SMART rules.

Passwords

All users of the school network have a secure username and password. There is a generic password for each child to enable them to access software and internet activities and tasks and allowing for monitoring of usage. The administrator password for the school network is available to the Head Teacher and it is kept in a secure place. Staff and pupils are reminded of the importance of keeping passwords secure as part of the curriculum.

Software/Hardware

All software is licensed and copies of licences are kept in the office. Software can only be loaded by ICT technician at the request of the Head teacher or Computing Subject Lead. Regularly updated software toolkits and Hardware audits are available to staff and software. See Schools Computing policy.

Managing the Network and Technical Support

The server and cabling are securely located in the Comms box in the stock room. A Computer technician from BTConnect is responsible for keeping the security of the network up to date with critical software updates.

Users have clearly defined access rights; pupils can access their documents and the pupil's folder. Teachers can access their documents, pupils' folder and the teacher's folder; they may also download/load additional software with permission of the Head teacher or Computing Subject Lead

All staff and pupils are required to log out when they leave a computer unattended. All users must report any suspicion or evidence of a breach of security to the Computing Subject Lead or the Head teacher.

Staff are permitted to use USB pens to store or transfer data, but these must be regularly checked for viruses and staff are aware that information stored on the pen can be monitored by the ICT co-ordinator or Head teacher.

Raising Staff Awareness

All staff are expected to promote and model responsible use of technology and digital resources. Training is provided within an induction programme for all new staff to ensure that they fully understand the school's Policy and Acceptable Use agreement.

The School Policy will be available to all staff and its importance explained. All existing staff, governors, regular visitors and supply staff will be asked to sign a Technology and Internet Safety Acceptable Use Agreement.

Digital Safety is discussed regularly at curriculum meetings and on the agenda for support staff and welfare meetings. Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Parents' attention will be drawn to the School's policy through a range of different ways. On the School website, the SMART rules for using the internet safely are displayed, there is a monthly newsletter, keeping them up to date with emerging digital social media the children may use and other useful information and links to additional digital safety web sites.

Parents will be asked to sign the Pupil's and Parent's ICT acceptable use agreement and read and sign image consent and conditions of use form.

Raising Governors' Awareness

The Subject Lead will liaise with the specific governors with responsibilities for, including Computing or Child Protection Governors to ensure they are kept up to date.

Standards and Inspection

The Policy should be regularly reviewed and approved by the Governing body ensuring robust safeguarding procedure is a main priority at St Mark's School. The policy is reviewed annually and all staff and governors are kept up to date and any changes or updates are added to the agenda of the next meeting e.g. Staff meeting, Governors curriculum committee meeting.

Any incidents will be recorded in the Incident log.

The policy and appendices, including the acceptable use agreements will be reviewed at least annually and will include reference to new trends and emerging technologies.

Updating the policy

This policy has been written by the school, building on Local Authority guidance and government guidance. It has been approved by governors.

Next Policy Review: March 2025

Appendix 1a

Staff, Supply Teachers, External Staff, Visitor and Governor Digital Safety Acceptable Use Agreement

Background and Purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times.

Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must.
Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements. The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care about the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.

• I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
• I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
• If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
• I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that permission has been granted by the head teacher in writing for each occurrence.
• I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.
• I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
• I will never download or install software unless permission has been given by the appropriate contact at school.
• I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.
• I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely. This includes locking laptop screens when leaving the room.
• Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
• I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children. These devices will be securely locked away with adequate password protection on them should they be accessed by an unauthorised person.
• Any school trips/outings or activities that require a mobile phone/camera will be provided by the school and any data collected on them will be used in accordance with school policies.
• At no point- will I use my own devices for capturing images/video or making contact with parents/carers.

User Signature

- I have read and understood the school digital safety policy.
- I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature: ___________________________________

Date: ___________________________________

Full Name: ___________________________________ (PRINT)

Post/Role: ___________________________________

Appendix 1b

Parent/Carer Digital Safety Acceptable Use Agreement

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies. This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting. The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

Parents/Carers

We ask parents and carers to support us by:

- Sharing good online behaviours with your child.
- Emphasising the importance of the Acceptable Use Statements/School's rules your child has agreed to.
- Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
- Explaining how to keep an appropriate digital footprint.
- Discussing what is and isn't appropriate to share online.
- Emphasising never to meet anyone online nor trust that everyone has good intentions.
- Reporting any concerns you have whether home or school based.
- Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

User Signature

- I have read and understood the school digital policy.
- I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature: ___________________________________

Print name: ___________________________________

Date: ___________________________________

Appendix 1c

EYFS Pupil, Parent/Carer Digital Safety Acceptable Use Agreement

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.

This is to be read through with your parents/carers and then signed to show that the e-Safety Rules have been understood and agreed.

- I ask before I use a tablet, computer or camera.
- I tap or click on things I have been shown.
- I check if I can tap/click on things I haven't seen before.
- I tell a grown-up if something upsets me.

Signed:______________________________(Pupil)

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and _____________________________________ [Print child's name] agrees to follow the Digital Safety rules and to support the safe use of ICT.

Parent /Carer Signature: ______________________________

Parent /Carer (Priant): ______________________________

Date: ___________________________

Appendix 1d

KS1 Pupil, Parent/Carer Digital Safety Acceptable Use Agreement

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.

This is to be read through with your parents/guardians and then signed to show that the Digital Safety Rules have been understood and agreed.

- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post to our blogs, use our email and other communication tools.

I understand this agreement and know the consequences if I don't follow it.

Signed:____ (Pupil)

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and ____________________________________ [Print child's name] agrees to follow the Digital Safety rules and to support the safe use of ICT.

Parent /Carer Signature: ______________________________

Parent /Carer (Priant): ______________________________

Date: ______________________________

Appendix 1e

KS2 Pupil, Parent/Carer Digital Safety Acceptable Use Agreement

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.
This is to be read through with your parents/carers and then signed to show that the Digital Safety Rules have been understood and agreed.

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice or that someone who isn't approved by the teacher is messaging.
- Before I share, post, reply to anything online, I will: T = is it true?
  H = is it helpful?
  I = is it inspiring?
  N = is it necessary?
  K = is it kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

Signed:____ (Pupil)

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and ______________________________________
[Print child's name] agrees to follow the Digital Safety rules and to support the safe use of ICT.

Parent /Carer Signature: ____________________________

Parent /Carer (Print): ____________________________

Date: ____________________________

Appendix 2

Digital Device and Website Incident Report

Date: ______________

Class: ______________

Incident and reason for investigation:

Details of first reviewer:

Name: ________________________________

Position: ________________________________

Signature: ________________________________

Details of second reviewer:

Name: ________________________________

Position: ________________________________

Signature: ________________________________

Name and location of device: ____

Review device and location: ____

WEBSITE ADDRESS/DEVICE	CONCERN

Action Taken:

Appendix 3

St Mark's CE Primary School

Image Consent Form

Dear Parent/Carer

We write to you today to inform you of the use of photographs and videos of the children at our school.

As you know, we regularly take photographs and videos of children at our school. These may be used for school brochures and on the school website. Photographs of individual and groups of children may be used in learning journeys, children's books and school displays.

The local media sometimes visit the school and as such, photographs may appear in the local paper to publicise a particular event r to celebrate a specific achievement. On occasions this may also result in publication on websites and/ or a feature in a television programme. Parent/Carers should note that website can be viewed throughout the world and just in the United Kingdom where UK law applies.

To protect your child's details, the school will not use the full names of children to accompany any photograph or video. However, we may use the Christian names and age of your child. If we or other members of the media do not use a photograph but are printing news about the school or individual achievement we will not use the full name of that pupil but may use a Christian name, age, class name or school name.

Parents, Carers, family members and friends are all invited into school to see school activities such as sports day, plays etc. It is therefore understandable that at these events many parents wish to take photos and/or videos. Those who attend such events need to be aware that any pictures and/or videos may contain images/footage of your child. We ask that these images are **NOT** shared in any way including social networking sites. Although the school does have Facebook and Twitter accounts, parents/cares should be aware that we have no way of policing or controlling what is shared on these sites and as such, ask that you refrain from placing such photographs and videos on any social networking website.

This form will be valid from the time you sign and date it. Although we continually look at updating our information you need to be aware that there may be an overlap on images on websites and in school brochures etc. when you child leaves school until such information is updated.

In order that we can protect your child's interests, and to comply with the Data Protection Act (1998) we ask that you sign and return this form as confirmation that you have read and understood the contents. If you have any questions or need clarification on anything please speak to Mrs Freeman before signing.

Name of child……

Name of Parent/Carer………

Signature ……………………………………………………………………………… Date ……………………………………………………

Relationship to child ………………………………………………………………

This information will be used on a computerized system. The school is registered under the Data Protection Act to keep such information.
Pupil data will be used for statutory returns to the Local Authority and registered Government Agencies