St Monica Primary School
Inspire – Endeavour – Achieve

E Safety & Internet

Usage Policy

(including Acceptable Use

Agreements)

Policy Statement and Guidelines

E Safety and Internet Usage Policy		Signed by the Chair of Governors:
Date of Issue:	Summer 2019	
Approved by Governing Body:	Summer 2019	
Review Date:	Summer 2020	

E Safety And Internet Usage

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's E safety policy will operate in conjunction with other policies including those for Email Security and Etiquette Guidance, Positive Behaviour and Anti-Bullying, Safeguarding, Child Protection, Mobile Phone, Data Protection, Image Consent form and Security.

Background - Why Is Internet Use Important?

The purpose of internet 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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and St Monica has a duty to provide pupils with quality internet access.

Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

How Does Internet Use Benefit Education?

Benefits of using the internet in education include

- access to world-wide educational resources including museums, libraries and art galleries
- rapid and cost effective worldwide communication
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of
- networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority
- access to learning wherever and whenever convenient
- greatly increased skills in Literacy

How Can Internet Use Enhance Learning?
- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of our pupils
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Good Habits

E safety depends on effective practice at a number of levels:
- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network standards and specifications.

Dangers to Consider

Some of the dangers children may face include
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The E safety policy that follows explains how we intend to do this.

E safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the E safety basics are in place.

Has the school an E-safety Policy that complies with CYPD guidance?	Yes
Date of latest update:	2019
The Policy was agreed by governors in:	Summer 2019
The Policy is available for staff at:	School website
And for parents at:	School website
The designated Child Protection Teacher/Officer is	Kathryn Bevan- Mackie
The E-safety Coordinator is:	Kathryn Bevan-Mackie
The E safety Governor is:	Natasaha Coutts
Has E-safety training been provided for both pupils and staff?	Yes
Do all staff sign an ICT Code of Conduct on appointment?	Yes
Do children sign an agreement about responsible IT use? Are parents sent a copy of that?	Yes from Years 2-6
Have school E safety rules been set for pupils?	Yes
Are these rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access	Yes
Has the school filtering policy been approved by the SMT?	Yes - annual review
Is personal data collected, stored and used according to the principles of the Data Protection Act 2018?	Yes

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Broadband monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- E safety co ordinator in school and the E safety governor will meet regularly to review monitoring

St Monica Primary School E Safety And Internet Usage Policy

Internet Access And Responsibility
- All staff must read and sign the **Staff Acceptable ICT Use Agreement** (Appendix A) before using any school ICT resource
- Parents are informed that pupils will be provided with supervised internet access.
- Parents will be sent a copy of the **Pupil Acceptable ICT Use Agreement** which their children will have read with their teachers and signed in class (Appendix B)
- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the E safety coordinator and network manager who will investigate and take appropriate action, liaising with broadband provider if necessary
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email & Online Collaboration
- Pupils may only use approved email accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive messages
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Pupils may must not access others pupil's accounts or files
- Whole class or group email addresses should be used in school
- Pupils must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the internet and have a clear idea of why they are using it.

- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses
- Pupils must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USBs should be virus scanned before use.
- Access in school to external personal email accounts may be blocked
- The forwarding of chain letters is not permitted

Social Networking
- At St Monica we block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old

Filtering
The school will work in partnership with Internet Service Provider to ensure filtering systems are as effective as possible.

Managing Emerging Technologies
- Emerging technologies will be examined for educational benefit and their risks assessed
- Mobile phones will not be used for personal use during lessons or formal school time on the school site. See our Mobile Phone policy
- The sending of abusive or inappropriate text messages or photos (sexting) is forbidden

Published Content & The School Website
- The contact details on the web site should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Information System Security
- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with our technical support team and broadband provider if necessary

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Please see our Data Protection policy.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the 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

Handling E safety Complaints
- Complaints of internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the head teacher
- These will be logged and dealt with as deemed appropriate by the head teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures
- Pupils and parents will be informed of the complaints procedure (See Making A Complaint – a guide for parents)

Communication Of E safety And Internet Usage Policy
Pupils
- Pupils will sign an Acceptable Use Agreement
- Rules for internet access will be posted in all classrooms
- Pupils will be informed that internet use will be monitored
- Pupils will be reminded of E safety rules regularly – especially when using the internet

Staff
- All staff will be given the E safety Policy and its importance explained
- Staff will sign an Acceptable Use Agreement
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents
- Parents' attention will be drawn to the E-safety Policy in newsletters, communication home and the school website
- Parents will receive a copy of their child's Acceptable Use Agreement

Appendices

Appendix A - Staff and Governor Acceptable Use Agreement

To ensure that all staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.

1. Aims & Background

This ICT user agreement covers the use of all digital technologies while in school: ie email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or Local Authority, or other information or systems processors.

This ICT user agreement also covers school issued equipment when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school.

This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute.

The school regularly reviews and updates with the assistance of the DPO, all user agreement documents to ensure that they are consistent with current school policies as listed at the end of the agreement.

2. User Requirements

School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures.

Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

a) I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body in the line of my employment.

b) I will set strong passwords, following advice provided by the school. I will change it frequently.

c) I will not reveal my password(s) to anyone.

d) I will not use anyone else's password if they reveal it to me and will advise them to change it.

e) I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.

f) I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols, and retention policy.

g) I will not engage in any online activity that may compromise my professional responsibilities.

h) I will only use the schools approved email system(s) for any school business.

i) I will only use the approved method/s of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business.

j) I will not support or promote extremist organisations, messages or individuals.

k) I will not give a voice or opportunity to extremist visitors with extremist views.

l) I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

m) I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head.

n) I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the School Office.

o) I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

p) I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other malware systems.

q) I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

r) I will follow the school's policy on use of mobile phones/devices at school

s) I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.

t) I will only I take or publish images of staff and students with their permission and in accordance the school's consent guidelines. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

u) I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.

v) I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two.

w) I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

x) I agree and accept that any computer or laptop or memory stick loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

y) I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.

z) I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

aa) I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

bb) I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

cc) I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.

dd) I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.

ee) I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

ff) I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.

gg) I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

3. Links with Other Policies

I understand that this user agreement is linked to the schools:

- Online and E-Safety Policy
- Email Security and Etiquette Guidance
- GDPR/Data Protection Policy
- Document Retention Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Safeguarding and Child Protection Policy

4. Agreement Form

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .... Date ....

Full Name .... (printed)

Job title / Role ....

Appendix B

Acceptable Use Agreement for KS1
- I will only use the internet or computer when a teacher or adult is with me
- I will only use my own login and password and I will not tell anyone else what it is
- I will not look at or delete other people's files
- I will not bring in memory sticks from home without permission
- If I see anything that upsets me, I will tell an adult
- I will not give out any details about me – like my name or address
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

Acceptable Use Agreement for KS2

- I will use the school computers and technology sensibly
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages on the computer
- I will not give out my personal information or arrange to meet anyone
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

Appendix C - Letter sent home to all pupils and their parents of KS2. KS1 will have same letter but with their Acceptable Use Agreement

Dear Parents
In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At St Monica we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children. Social networks have no place in our school and so school staff should not be approached by pupils or parents online or invited to join.

Your child has read the following **Acceptable Use Agreement** in class with their teacher. Once they have fully understood them all, your child has signed their name to agree to stick by them. Please read them again at home with your child to show your support of the school in this important aspect of our work. Thank you.

- I will use the school computers and technology sensibly
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages on the computer
- I will not give out my personal information or arrange to meet anyone
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

Appendix D

Use of Communication and Information Technology In School
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 / disadvantages:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	*							*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones				*				*
Use of school hand held devices eg iPads	*						*	
Use of personal email addresses in school, or on school network	*							*
Use of chat rooms/facilities				*		*		
Use of instant messaging				*		*		
Use of social networking sites				*				*
Use of blogs				*		*		
Use of secure learning platforms to collaborate	*				*			

When using email the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email or electronic message that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and parents must be professional in tone and content
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails

and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.