1Excellence
Multi Academy Trust

Whatever you do, work at it with all your heart.
Colossians 2:23

St Mark's C of E Primary School

E-Safety Policy

Approved by governors: February 2019

Reviewed: February 2019

To be reviewed: January 2020

Mission Statement

At St Mark's C of E Primary School we will:

- Welcome everyone
- Build Christian values and worship into our teaching
- Establish strong links between home, school and community
- Endeavour to reach our full potential and celebrate our achievements
- Care for, encourage and respect each other
- Support each other to stay safe, healthy and make a positive contribution to our World

Our school is a place where every person has the right to be themselves and to belong and learn in a safe and happy environment. Everyone at our school is equal and treats each other with respect and kindness. We do not tolerate bullying.

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

The E safety co-ordinator is Mrs Dacombe/Miss Boagey

The safeguarding officer is Mrs V Hall Head Teacher

The designated teachers for child protection are Mrs V Hall, Mrs D Hindson, Mrs P Thornton, Mrs D Dacombe, Mrs D Carr

Safeguarding Director is Mrs F Williams.

Headteacher:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and Governing body are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Co-ordinator :

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor (Safeguarding appointed person) to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The ICT Technician / ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Stockton Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network/ email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator/Headteacher for investigation/action/ sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator/Headteacher for investigation/action/ sanction

- digital communications with students/pupils (email/voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students/pupils understand and follow the school e-safety and acceptable use policy
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection:
Child protection person should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student/Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

    - Pupils will, alongside parliament, write their own set of e safety rules and sign them to agree to adhere to them.

Parents / Carers:
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/ local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing the Student/Pupil Acceptable Use Policy
- accessing the school website/pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users
Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Use of mobile devices
No personal mobile phone, tablets or personal devices should be used in school when the children are present. If devices are to be used in school it is under the head teachers discretion and direction, and not in the presence of pupils.

Policy Statements

Education – students/pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating students/pupils to take a responsible approach. The education of students/pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. A half day is designated each half term to e safety.
- Students/pupils should 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
- Students/pupils should be helped to understand the need for the student/pupil to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers
Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. 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. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
    - Parents information session

Education & Training – Staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by BECTA/LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Coordinator will provide advice/guidance/training as required to individuals as required

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub committee/group involved in ICT/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.
- All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames.
- The “administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- Users will be made responsible 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.
- The school maintains and supports the managed filtering service provided.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager, e-safety co-ordinator and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the Network Manager.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations / portable devices. (see School Personal Data Policy Template in the appendix for further detail)
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students/pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students/pupils should 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
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/ pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

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

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students/pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email 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 students/pupils or parents/carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while students/pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students/pupils 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.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the

policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The Headteacher will take appropriate action, informing official channels.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students/pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email,etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

St Mark's C of E Primary School

Primary Pupil Acceptable Use

Agreement/E-Safety Rules

To be added when children have updated them.

St Mark's C of E Primary School eSafety Incident Log

Details of ALL eSafety incidents to be recorded on CPOMS and all SLT need to be alerted.