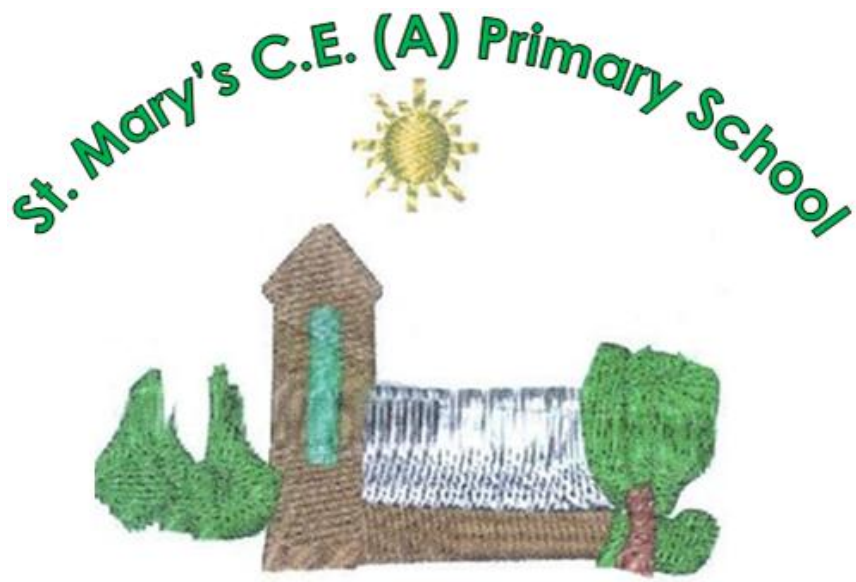

St. Mary's C.E. (A) Primary School

Greenfield

E-Safety Policy 2017

'We enjoy learning and achieving in a Christian environment'

ST MARY'S' C.E. (A) PRIMARY SCHOOL GREENFIELD

E-SAFETY POLICY 2017

Mission Statement:

'We enjoy learning and achieving in a Christian environment.

Every Child Matters at St. Mary's

St. Mary's wants every child to be healthy, stay safe, enjoy and achieve, make a positive contribution and achieve economic well-being. This policy has been written with careful consideration of the Every Child Matters Agenda.

Healthy School

St. Mary's is a Healthy School with healthy attitudes embedded in the curriculum and extra-curricular activities. Children are encouraged to be active and maintain healthy relationships with their peers and adults as well as making choices about healthy lifestyles.

Building Learning Power Statement

At St. Mary's, we encourage all pupils to build their own learning power. Building Learning Power emphasises the development of lifelong learning values and skills. We aim to ensure that all children develop persistence and curiosity for learning and become adventurous risk takers who are not afraid of the 'don't know' state of mind. At St. Mary's, children will develop the ability to take responsibility for their own learning and self assess and be able to articulate themselves as a learner. They will have the opportunity to develop the ability to know what's worth learning, know how to face confusion and know the best learning tool for the job.

Introduction

- This Policy was approved by The Governing Body on 26th January 2017 and will reviewed in Spring 2020 in accordance with the Policy Review Cycle.

What is E-Safety?

E-Safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies (such as games consoles and wireless technology), both in and out of school. It highlights the need to educate children about the benefits, risks and responsibilities of using information technology.

- E-Safety concerns safeguarding children and young people in the digital world.
- E-Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more about education about the risks as well as the benefits so users can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

E-Safety is part of the 'duty of care' which applies to everyone working with children. The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that E-Safety is an ever growing and changing area of interest and concern.

Why do we need an E-Safety Policy?

Pupils interact with new technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger. School must decide on the right balance between controlling access, setting rules and educating pupils for responsible use.

At St Mary's we understand the responsibility to educate our pupils on E-Safety issues, teaching them the appropriate behaviours and thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the classroom.

This document describes strategies to help to ensure responsible and safe use for both staff and children. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. There are no straightforward or totally effective solutions and staff, parents and children must remain vigilant. They must also know what to do if they do come across inappropriate material.

Both this policy and the Acceptable Use Policy (for all staff, governors, and pupils) include both fixed and mobile internet technologies provided by the school (including such technology as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, voting systems, digital video equipment, etc) and technologies owned by pupils and staff, but brought onto school premises (including such technology as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and responsibilities

The Headteacher, as Designated Safeguarding Lead, is responsible for ensuring the safety (including E-Safety) of all members of the school community, though the day to day responsibility for E-Safety can be delegated.

An E-Safety Leader/Computing Coordinator will be appointed who, working with the, Designated Safeguarding Lead will have overall responsibility for child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

All staff will work with the E-Safety Leader to implement and monitor the E-Safety policy and the AUP (Acceptable Use Policy).

Governors

- Approve and review the effectiveness of the E-Safety Policy
- Nominate a governor to act as E-Safety link
- The nominated governor for Safeguarding and Child Protection is Reverend Jenny Degg, Chair of RE Worship and Pastoral Committee.
- E-Safety Governor works with the E-Safety Leader to carry out regular monitoring and report to Governors

Head Teacher and Senior Leaders

- Ensure that all staff receive suitable CPD to carry out their E-Safety roles
- Create a culture where staff and learners feel able to report incidents
- Ensure that there is a system in place for monitoring E-Safety
- Follow correct procedure in the event of a serious E-Safety allegation being made against a member of staff or pupil
- Inform the local authority about any serious E-Safety issues
- Ensure that the school infrastructure/network is as safe and secure as possible
- Ensure that policies and procedures approved within this policy are implemented
- Use an audit to annually review E-Safety with the school's technical support

E-Safety Leader/Computing Co-ordinator

- Log, manage and inform others of E-Safety incidents
- Lead the establishment and review of E-Safety policies and documents
- Ensure all staff are aware of the procedures outlined in policies relating to E-Safety
- Provide and/or broker training and advice for staff
- Attend updates and liaise with the LA E-Safety staff and technical staff
- Meet with Senior Leadership Team and E-Safety Governor to regularly discuss incidents and developments
- Coordinate work with the school's designated Child Protection Coordinator

Teaching and Support Staff

- Participate in any training and awareness raising sessions
- Read, understand and sign the Staff AUP
- Act in accordance with the AUP and E-Safety Policy
- Report any suspected misuse or problems to the E-Safety Leader
- Monitor computing activity in lessons, extracurricular and extended school activities

Pupils

• Read, understand and sign the Pupil AUP and the agreed class internet rules
• Participate in E-Safety activities, follow the AUP and report any suspected misuse
• Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school

Parents and Carers

• Endorse the Pupil AUP
• Discuss E-Safety issues with their child(ren) and monitor their home use of computing systems (including mobile phones and games devices) and the internet
• Access the school website in accordance with the relevant school AUP
• Keep up to date with issues through newsletters and other opportunities
• Inform the Headteacher of any E-Safety issues that relate to the school

Technical Support Provider

• Ensure the school's computing infrastructure is as secure as possible
• Ensure users may only access the school network through an enforced password protection policy for those who access children's data
• Maintain and inform the Senior Leadership Team of issues relating to filtering
• Keep up to date with E-Safety technical information and update others as relevant
• Ensure use of the network is regularly monitored in order that any misuse can be reported to the E-Safety Leader for investigation
• Ensure monitoring systems are implemented and updated
• Ensure all security updates are applied (including anti-virus and Windows)

Education of pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to E-Safety' School Inspection Handbook - OFSTED 2014

A progressive planned E-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Within this:

• Key E-Safety messages are reinforced through assemblies and Safer Internet Week (February), anti-bullying week (November) and throughout all lessons.
• Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
• Pupils are guided to use age appropriate search engines for research activities.
•Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
• In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches. Staff pre-check any searches.
• Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.

• Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
• Pupils will write and sign an AUP for their class [which might be agreed class rules] at the beginning of each school year, which will be shared with parents and carers
• Pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing E-Safety risks at home, reinforcing key messages about E-Safety and regulating their home experiences. The school supports parents and carers to do this by:
• providing clear AUP guidance which they are asked to sign with their children and regular newsletter and website updates
• inviting parents to attend activities such as E-Safety week, E-Safety assemblies or other meetings as appropriate.

Training of Staff and Governors

There is a planned programme of E-Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUP. This includes:
• An annual audit of the E-Safety training needs of all staff.
• All new staff receiving E-Safety training as part of their induction programme.
• The E-Safety Leader receiving regular updates through attendance at LA training sessions and by reviewing regular E-Safety newsletters from the LA.
• This E-Safety Policy and its updates being shared and discussed in staff meetings.
• The E-Safety Leader providing guidance and training as required to individuals and seeking LA support on issues.
• Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
• The school will follow procedures in place to support anyone in the school community affected by cyberbullying.
• All incidents of cyberbullying reported to the school will be recorded.
• The school will follow procedures to investigate incidents or allegations of cyberbullying.
• Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
• The school will take steps where possible and appropriate, to investigate the incident with support from the LA.

Prevent

The Headteacher as Designated Safeguarding Lead has overall responsibility for the schools implementation of *Prevent* Strategy and Prevent Safeguarding in school.
The local authority provides web filtering that is double check by the in house ICT Technician. This includes, appropriate filtering to prevent access to terrorist or extremist material. Any inappropriate content and/or information that may give cause for concern, is reported to the ICT Technician

Technical Infrastructure

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

• The School computing systems are managed in ways that ensure that the school meets E-Safety technical requirements

• There are regular reviews and audits of the safety and security of school computing systems.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

- the downloading of executable files by users
- the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
- the installing programs on school devices unless permission is given by the technical support provider or Computing Coordinator
- the use of removable media (e.g. memory sticks) by users on school devices.
- the installation of up to date virus software

• Access to the school network and internet will be controlled with regard to:

- users having clearly defined access rights to school computing systems through group policies
- users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details
- users must immediately report any suspicion or evidence that there has been a breach of ecurity
- an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this E-Safety policy
- Key Stage 1 pupils' access to the internet will be by adult demonstration with directly supervised access to specific and approved online materials
- Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and activities which will be adult directed

• The internet feed will be controlled with regard to

- the school providing a managed filtering service provided by an educational provider
- the school monitoring Internet use.
- requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged

- requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged
- any filtering issues being reported

• The computing system of the school will be monitored with regard to:
  - the school computing technical support regularly monitoring and recording the activity of users on the school computing systems
  - E-Safety incidents being documented and reported immediately to the E-Safety Leader who will

arrange for these to be dealt with immediately in accordance with the AUP

Data Protection

The school's Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The school will:

• 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

• ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, and to provide information about the school on the website. The school will:

• When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.

• Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.

• Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.

• Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs.

• Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.

• Not publish pupils' work without their permission and the permission of their parents.

• Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

• with respect to email
  - Ensure that all school business will use the official school email service.
  - Ensure that any digital communication between staff and pupils or parents and carers (email, chat, etc) is professional in tone and content.

- Make users aware that email communications may be monitored.
- Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Provide whole class or group email addresses where necessary.
- Teach pupils about email safety issues through the National Curriculum and implementation of the AUP.
- Ensure that personal information is not sent via email.
- Only publish official staff email addresses.

• with respect to social media (e.g. Youtube, Facebook, Twitter, blogs) and personal publishing

- enable online learning opportunities to make use of age appropriate educationally focused sites that will be moderated by the school
- control access to social media and social networking sites in school
- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Leadership Team
- ensure that any digital communication between staff and pupils or parents and carers is always professional in tone and content
- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with Teaching Standards 2012
- staff are advised that no reference should be made to pupils, parents/carers or school staff
- advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- register concerns regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- support staff to deal with the consequences of hurtful or defamatory posts about them online
- inform the staff that in the case of a Critical Incident they should not make any comment on social media without the permission of the senior management team

• with respect to personal publishing

- Teach pupils via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their

parents and carers, particularly when concerning pupils' underage use of sites.
    - Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction.
    - Outline safe and professional behaviour.

• with respect to mobile telephones

- inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher
- inform staff that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team
- inform all that personal devices should be password protected
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- inform visitors of the school's expectations regarding the use of mobile phones
- allow pupils to bring mobile phones into school at their own risk but only for use at specified times and for approved activities. Phones must be handed into the office during school hours and will be returned at the end of the day unless a medical need.
- maintain the right to collect and examine any phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection

How will Emerging Technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers.

At St Mary's we will ensure that we stay up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How will the policy be introduced to pupils?

As children's perceptions of the risks of internet use will vary, E-Safety rules may need explanation and discussion. Children should be reminded through the display of E-Safety Rules at the point of Internet use. Posters which state reminders of what responsible use of internet technology is are posted around school.

A module on responsible Internet use is included in the PSHE programme of study for year 5 and year 6 covering both school and home use of the internet.

The annual E-Safety week will also be used to address the issue of online safety, with information available on the school website.

This policy was written following the SWGfL, Kent County Council, South Gloucestershire County Council E-Safety policy templates.

Approved by:  **Chair of RE, Worship and Pastoral Committee**

Date: 26th January 2017

Review Date: Spring 2020