ST. MARY'S SCHOOL

(to include EYFS)

Safeguarding Online Safety Policy

Date: September 2016

Review date: August 2017

Mission Statement

At St. Mary's we aim to provide an inspiring, enjoyable educational experience where all children can develop their talents, whether academic, creative or sporting. Our school is a place where everyone is treated equally, encouraged and respected. We are committed to our school being a safe and inclusive place where learning is nurtured and confidence and self-esteem is grown in a happy, caring and stimulating environment. Ultimately, we want our pupils to develop a love of learning for life.

St Mary's School believes that the use of information and communication technologies in schools brings great benefits. The school recognises e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

Contents:

1. Who will write and review the policy?

- The e-safety policy is written, reviewed and co-ordinated by Rob Harmer (Head and IT co-ordinator) and Kate Bodle (Designated Safeguarding Lead). Any questions or worries should be directed to Rob or Kate.

2. Why is Internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education. St Mary's has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
    - 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 functions.
    - Internet access is an entitlement for students who show a responsible and mature approach to its use.

3. How does Internet use benefit education and learning?

- The school's Internet access will be designed to enhance and extend education;

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- St Mary's will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to 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, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

The Internet can help pupils and staff with:

- access to worldwide educational resources and information;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

4. How is security maintained?

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed.

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

5. How is email managed?

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Whole class or group email addresses will be used in school for communication outside of school.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Schools may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team.
- Staff should only use school email accounts to communicate with parents of pupils in school or with other staff members
- Staff should not use personal email accounts during school hours or for professional purposes

6. How is published content managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is suitable for publication
- Images of a pupil should not be published without the parent's or carer's consent
- Pupils are taught the reasons for publishing personal information and images online

7. How is social networking, social media and personal publishing managed?

- The school will control access to social media and social networking sites.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Headteacher. Staff should be advised not to run social network spaces for pupil use on a personal basis.
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

8. How is filtering managed?

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of information.
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- Key loggers record all text sent by a workstation and analyse it for patterns. False positives will require manual checking.
- If staff or pupils discover unsuitable sites, it must be reported Rob Harmer or Kate Bodle

9. How is personal data protected?

Personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

10. How is Internet access authorised?

- At Key Stage 1 and 2 access to the Internet will be by adult demonstration with supervised access to specific, approved online materials.
- Parents are informed that pupils will be provided with supervised Internet access

11. How are e–Safety complaints handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the headteacher.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will work in partnership with staff to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

12. How is Cyberbullying managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by Cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

13. How is the policy introduced to pupils?

- In lessons, the pupils are consistently reminded of the e-safety rules and posters displayed on the IT Laptop trolley. At the beginning of each year the children are reminded of these expectations and through the CEOP resources the children learn about situations which could occur online and how to handle these situations.

  Useful e–Safety programmes include:

- Think U Know: ***www.thinkuknow.co.uk***
- Childnet: ***www.childnet.com***
- Kidsmart: ***www.kidsmart.org.uk***
- Safe Social Networking: ***www.safesocialnetworking.com***

14. How is the policy discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is essential.
- Each staff member is alerted to his/her responsibility in the delivery of ICT lessons (this is

displayed in the IT room as a reminder)

15. How is parents' support enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
- Parents and pupils will be requested to sign an e–Safety/internet agreement (see appendix)

Policy revised September 2016 (to be reviewed August 2017)

Appendix:

ST. MARY'S SCHOOL

COMPUTER USE AGREEMENT FOR STUDENTS and PARENTS September 2016

The document is comprised of this cover page and two sections:

Section A:

- Computer Use Agreement for St. Mary's School and Internet Safety Rules including explanatory notes for parents

Section B:

- Parent and Student Computer Use Agreement Form

Instructions for Parents

1. We are sure that as Parents you are only too aware of the way the world of communication has changed. What was unthinkable just a few years ago becomes reality in a flash and keeping up with all the benefits and dangers this brings becomes a challenge. Our firm belief is that the best way of maximising the benefits whilst minimising the dangers is for Parents, Pupils and the School to have a common understanding around the use of ICT.

We would like you to read the Computer Use Agreement and the Internet Safety Rules carefully. If help is needed to understand all the language, or there are any points you would like to discuss with the school, let the school know as soon as possible. It is the intention of our school to make available "ICT awareness sessions for parents".

2. Discuss the Internet Safety Rules with your child and think through how you manage this within or outside your home.

3. Both you and your child should sign the Computer Use Agreement Form and return that page to the school office.

4. Please keep Section A for future reference.
(The term 'Parent' used throughout this document also refers to legal guardians and caregivers)

Important terms used in this document:
*(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'.*
*(b) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined) below.*
*(c) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audioplayers/receivers (such as portable CD and DVD players), and any other, similar technologies as they come into use.*

SECTION A – INTERNET SAFETY AND THE SCHOOL COMMUNITY

COMPUTER USE AGREEMENT - ICT Safety Policy at St. Mary's School

The values promoted by St. Mary's School include respect for yourself and others in the school community and a commitment to enabling everyone to achieve their personal best in an environment which is physically and emotionally safe. The measures outlined in this document ensure the internet safety of the school is based on these values.

The school's computer network, internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at St. Mary's School and to the effective operation of the school. However, it is essential that the school endeavours to ensure the safe use of ICT within the school community.

Internet safety use agreements include information about obligations and responsibilities and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the school environment. The overall goal of the school in this matter is to help keep the school community safe by creating and maintaining an internet safety culture which is in keeping with the values of the school.

1. ICT Safety Policy

1.1. All staff and students, whether or not they presently make use of school ICT, will be issued with a Computer Use Agreement. Parents are asked to read these pages carefully and return the signed Agreement form in Section B to the school office for filing. A copy of this signed form will be provided on request.

1.2. Parents are asked to keep the other pages of the Agreement for later reference

1.3. The school encourages anyone with a query about the Agreement to contact staff.

2. Requirements regarding appropriate use of ICT in the school learning environment

In order to meet the school's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the school:

2.1. The use of the school's computer network, internet access facilities, computers and other school ICT equipment/devices is limited to educational purposes appropriate to the school environment.

2.2. The school has the right to monitor, access, and review all the use detailed in 2.1. This includes all emails sent and received on the school's computers and/or network facilities, either during or outside school hours.

2.3. The use of any privately-owned ICT equipment/devices on the school site, or at any school related activity, must be appropriate to the school environment. Such equipment/devices could include a laptop, desktop, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate should check with their teacher.

2.4. When using the internet, it may not always be possible for the school to filter or screen all material. However the school will attempt to filter as much dangerous, illegal or inappropriate content as is possible.
However, the expectation is that each individual will make responsible use of such systems.

3. Monitoring by the school

3.1. The school has the capacity to monitor traffic and material sent and received using the school's ICT infrastructures. From time to time this may be examined and analysed to help maintain a safe school environment.

3.2. The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.
However, as in 2.4., the expectation is that each individual will be responsible when using ICT.

The sections below are designed to provide a guide to the rules covered by this Use Agreement, and to help you discuss the rules with your child. Teachers will also go over this section with students.

1. I must have a Use Agreement signed by me and by my parent before I am allowed to use the school ICT equipment.
All students, regardless of age or ability, must have a Use Agreement signed by their parent and those in Year 4 and above must sign their use agreements along with their parents. Use Agreements are becoming accepted as an essential part of ICT safety policy within programmes for schools and other organisations, including businesses.

2. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.
This helps children and young people to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work

through an issue and so avoid the student making an unwise decision which could lead to serious consequences. Young children need on going guidance to help them become safe and responsible users of ICT.

3. I will follow the internet safety rules, and will not join in if others are being irresponsible.
Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major problem. Often children become involved in these acts through peer pressure without thinking of the consequences.

4. I will not use the internet, mobile phones or any other ICT equipment at anytime to be mean, rude, offensive, or to harass any members of the school community like students and staff, while enrolled in the school.
The basic principles of politeness and respect extend to the use of ICT. If I come across inappropriate material I will not show it or share it with others.

5. If I accidentally come across mean, rude or dangerous material, I will tell the teacher straight away, without showing any other students.
Because anyone at all can publish material on the internet, it does contain material which is inappropriate and in some cases illegal. The school has taken a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they find something which they suspect may be inappropriate encourages critical thinking and helps children to take responsibility for their actions and keep themselves and others safe.

6. If I am not feeling safe at any time while using the ICT equipment, I will tell the teacher straight away.
Our school strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a child to feel unsafe could include: contact being made by a stranger through email or text message, the presence of 'scary' images on a computer screen, and/or misconduct by other students. Staff need to be made aware of such situations as soon as they occur to ensure the school can respond immediately.

7. If I am sharing a computer with someone else, I share the responsibility for how it is used. If there is a problem, I will tell the teacher immediately.
Students often work together at a single computer. Any misuse of the computer can be traced back to whoever was logged on at the time. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.

8. I will check with the teacher or my parent before giving anyone information about myself or others when using the internet or a mobile phone – this includes home and email addresses and phone numbers.
This reduces the risk of your child, or other children being contacted by someone who wishes to upset or harm them or use their identity for purposes which might compromise their privacy.

9. I will not be careless, try to damage, or steal any school ICT equipment.

10. I will not try to stop the network or any other equipment from working properly or change, delete other people's work without their permission. I will not try to change screensavers, desktop backgrounds, themes or hardware settings without the teacher's permission.

11. If I accidentally break something, or I find it broken when I start to use it, I will tell a teacher straight away.

12. I will not print anything without the permission of the teacher.

13. I will not download any files such as music, videos, or programmes without the permission of the teacher, even if they are for school work. If I am unsure, I will ask the teacher first.
Many files available on the internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain malicious content such as viruses, or spyware. Some files may contain inappropriate or illegal material.

14. I must have a letter from home, requesting permission from school, before bringing any disk or other ICT device from home, unless it is part of my normal school equipment. If I am given permission, then I must use that ICT sensibly.
The devices referred to in this rule may include flash memory devices, iPods, MP3 players or mobile phones. Any students bringing such devices from home are asked to use them sensibly. This applies to the school site and any school-related activity.

15. I am aware the teacher can check any disk or ICT device (including all disks, memory storage devices, media players, cameras and mobile phones) I bring from home, before I use it with school equipment. I understand that viruses can be transferred to and from the school and accept there is no liability on behalf of the school should my personal or home equipment be compromised.
This rule is designed to protect the school's online security and equipment from viruses which can easily be transferred using disks

or other storage devices such as USB sticks or memory cards. If your child is using a disk or other device to transfer work between home and school, it should be freshly formatted, or 'blank', before use. This may also stop any of your own personal material from finding its way onto the school's equipment. Even though every effort is made to keep school equipment virus-free, you should scan your child's disk or device for viruses before they use it again with your home computer.

16. I will not bring software or games from outside school to use on school equipment.

Installing software from home may cause conflicts with the software installed by the school. Our school must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software.

17. I will acknowledge where work has come from if I have copied it from somewhere.

The internet has allowed easy access to a huge range of information which can be incorporated into students' work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. The value to students' learning is questionable if they have not thought through this information themselves.

18. Wherever I have a personal username, email address or login I will not share it with other people

It is very important that students learn the necessity of security awareness at an early age. Allowing others to gain access to their personal sites or information can leave themselves open to others misusing the internet in their name.

19. I will abide by the Mobile Phone Policy set out below and also not use or keep on my person mobile phones/sim card devices during my time in school.

Making the most of these rules

You might like to take this opportunity to have a discussion with your child about their general use of ICT whether in or out of school. It helps keep children safe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are (for example at home, at school, or at a friend's house), or who they are with.

Mobiles Phones at St. Mary's School

Our school policy regarding mobile phones is that children are not allowed to bring them to school unless they have permission from their parents and this has been discussed and agreed by the school. If permission has been granted they are required to hand them into the school office before registration, collecting them again at the end of the school day. Should parents wish to contact their child during the school day they may ring the office and we will arrange to get a message to the child.

SECTION B –

ST. MARY'S SCHOOL COMPUTER USE AGREEMENT

To the Student and Parent:

1. Please read this page carefully as it includes information about your responsibilities under this agreement.

2. Complete and sign the appropriate section.

3. Detach and return this section to the school office.

*4. Keep **Section A** for your future reference.*

Our School will:

• do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the internet or school ICT equipment/devices at school or at school related activities.

• work with children and their families to encourage and develop an understanding of the importance of internet safety through education designed to complement and support the Computer Use Agreement. This includes providing children with strategies to help keep themselves safe on the internet.

• keep a copy of this signed use agreement form on file.

• respond to any breaches in an appropriate manner.

• welcome enquiries from parents or students about internet safety issues.

Student's section

My responsibilities include:

*• **I will read** this Computer Use Agreement document carefully with my parent.*

*• **I will follow** the internet safety rules and instructions whenever I use school ICT.*

*• **I will have no involvement** in use of ICT which could put me or other members of the school community at risk.*

*•**I will be respectful** of other students and staff when I use the internet outside of school.*

*• **I will take proper care** when using computers and other school ICT equipment.*

*• **I will keep** Section A of this document somewhere safe so I can read it again later.*

*• **I will ask** my teacher or my parents if I am not sure about something to do with this Agreement. I have read and understand my responsibilities and agree to follow the Computer Use Agreement. I know that if I breach this use agreement there may be serious consequences.*

Name of student: ..... ***Class:*** .....

Signature: ..... ***Date:*** .....

Section for parent

My responsibilities include:

*• **I will read** this Computer Use Agreement document and discuss the rules with my child*

*• **I will ensure** this Agreement is signed by me and my child and returned to the school.*

*• **I will support** the school's internet safety programme by encouraging my child to follow the internet safety rules and to always ask the teacher if they are unsure about any use of ICT*

*• **I will contact** the Head or other staff to discuss any aspect of this Use Agreement which I might want to learn more about. I know I am welcome to do this at any time.*

I have read this Computer Use Agreement and am aware of the school's initiatives to maintain a safe learning environment and the responsibilities involved.

Name of Parent: .....

Signature: ..... ***Date:*** .....

I am/am not interested in ICT awareness sessions for parents (delete as applicable)

Signed:

Head Teacher: Rob Harmer

Person taking responsibility for monitoring E safety is: Kate Bodle & Rob Harmer