St Mary's C of E (Aided) Primary School, Pulborough

A Christ-centred school with a child-centred curriculum

E-SAFETY POLICY

At St Mary's C of E Primary School we take the safety of our pupils very seriously. E-safety involves pupils, staff, governors and parents making the best use of technology, information, training and this policy to create and maintain a safe online and computing environment for St Mary's Primary School.

As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly – when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or even illegal.
To ignore e-safety issues could ultimately lead to significant gaps on child protection policies, leaving children and young people vulnerable. (Safeguarding Children in a Digital World, BECTA, 2006)

1. E-Safety at St Mary's C of E Primary School:

This policy forms part of the School Improvement Plan and links to other policies such as ICT, child protection, behaviour and anti-bullying. It has been created with advice taken from a number of local authorities (West Sussex, Brighton and Hove, Kent and Sheffield) and also government guidance.
The e-safety coordinator is Mrs. Vicki Smith and they work closely with other members of staff responsible for child protection. This policy has been agreed by the senior leadership team and approved by the governors.
This policy will be reviewed annually as part of the safeguarding review.

2. Teaching and Learning at St Mary's C of E Primary School:

2.1 The importance of internet use

The purpose of the internet 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. The internet is an essential tool of the 21st century in all walks of life, including business and leisure; therefore schools have a duty to provide pupils with quality internet access as part of their learning experiences.

- The school internet access is designed expressly for pupil use and includes appropriate content filters.
- Pupils are given clear objectives for internet use and taught what is acceptable and what is not.
- Staff will give pupils online activities to enhance learning that are planned for their age and maturity.
- Pupils are educated in the effective use of the internet for research, including the skills of evaluation.

- When children are directed to websites for use at home they will have been checked for appropriateness by the teacher setting the learning.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught the importance of cross checking information before accepting its accuracy.
- As part of the new computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These topics include how to use a search engine, our digital footprint and cyber bullying.

3. Managing Internet Access at St Mary's C of E Primary School:

3.1 Information system security

- Security strategies are reviewed regularly in conjunction with West Sussex County Council and virus protection is updated on a regular basis by the school IT technician.
- Any portable devices should have a virus check before being used in school.
- The school server is backed up each night and if any administrator account passwords become known they will be changed straight away.
- All personal data sent via the internet will be secured or encrypted. Computers, including mobile devices, may not be connected to the school network, physically or wirelessly, without specific permission.
- Personal data, staff or pupils, should not be held on the school server without specific permission and any files held on the server will be regularly checked. No software is to be added or removed from the school network; any software to be added or removed may only be done so by the IT technician.

3.2 Email

- Pupils must only use approved email accounts on the school system. Access to personal email accounts is blocked.
- Pupils must immediately tell an adult if they receive offensive email.
- In any email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated with care and attachments not opened unless the author is known.
- The forwarding of chain letters is not allowed. All chain letters, spam, advertising and emails from unknown sources will be deleted without opening or forwarding.

3.3 Published content and school website

- The contact details on the school website are the school address, email and telephone number. Staff and pupils' personal details are not published.

- The head teacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.

3.4 Publishing of pupil images

- Photographs that include pupils will be selected carefully with the permission of parents / guardians
- Pupils full names will not be used anywhere on the school website or other online space, particularly in association with photographs.
- Pupils work will only be published on the website with permission of the pupil and parents / guardians.
- Parents are clearly informed of the school policy on image taking and publishing, both on the school and independent electronic devices.
- Written permission will be kept for pupils whose parents have allowed images to be published on the school website.

3.5 Social networking

Social networking internet sites provide facilities to chat and exchange information online. The online world is very different from the real one with the temptation to say and do things that would normally be said and done in face to face situations.

- The use of social networking sites in school is not allowed and will be blocked or filtered.
- Pupils are taught not to give out personal details of any kind that may identify themselves, other pupils, their school or location. This also includes photographs and videos.
- Pupils and parents will be advised that the use of social network sites outside of school is inappropriate for primary school aged children.
- Pupils are encouraged to only interact with known friends, family and staff over the internet and deny access to others.
- Parents, pupils and staff are advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.
- Pupils are taught how to use messaging with the virtual learning environment (Moodle) which is moderated by staff.

3.6 Mobile phones

Smartphones have access to the internet and picture / video messaging. Whilst these are advanced features, they present opportunities for unrestricted access to the internet and sharing images. There are risks of mobile bullying or inappropriate contact.

- Pupils are not to bring mobile phones to school unless given permission by the head teacher where parents have asked for permission for the phone to be present for safety / precautionary use. Pupil phones should be handed to the head teacher until home time.

- The sending of abusive or inappropriate text messages is forbidden.
- Staff should not use their own personal mobile phones to contact parents. The school phone should be used.
- Staff and visitors are not permitted to use their phones the classroom. Staff should turn off their phones, or put onto silent mode and store in a safe place away from children.
- Staff may use their mobile phone in the staffroom or office to make calls at break times away from pupils. Consideration should be given to other people in these areas when using phones.
- Parents may not use their mobile phones on school trips to take photographs of their own children or other children.

3.7 Cameras and video

Although most cameras are not directly linked to the internet, the images can easily be transferred.

- Pupils will not use cameras unless authorised by staff.
- Publishing of photographs and videos will follow the guidelines set out in sections 3.3 and 3.4 of this policy.
- Parents may use cameras to take images of their own children in school plays / assemblies when the head teacher gives permission but they must take images of other children. Images of children taken in school must not be shared on social networking sites.
- Photographs taken by parents must not be published in any manner; they are for private retention only.

4. Managing emerging technologies

Technology is fast changing and school will endeavor to keep up with new technologies as much as possible within the financial constraints that schools are faced with. As new technology comes to the forefront, school will consider it with regards to the educational benefit that it could bring. A risk assessment will be carried out before use in school is allowed.

- The senior leadership team is aware that new technologies such as mobile phones with wireless technology can bypass school filtering systems and present a route to undesirable material and communications. Mobile phones will not be used in lessons or formal school time.

5. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

6. Assessing risks

The school will take all reasonable precautions to ensure that the users access only appropriate material. However, due to the global and connected nature of the internet, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor West Sussex County Council can accept liability for the material accessed, or any consequences resulting from internet use.

- The school will audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimize risks will be reviewed regularly.

7. Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the head teacher or a senior member of staff in their absence.
- Any complaint about staff misuse must be referred to the head teacher or governing body.
- Complaints of a child protection nature will be dealt with in accordance with school protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be help with Sussex Police to establish procedures for handling potentially illegal issues.

DATE: Spring 2014
REVIEW DATE: Spring 2015