E-Safety Policy

Within our tradition as a Church of England (VA) Primary School, we are committed to making St Mary and St John an inclusive environment, fostering curiosity, spirituality, creativity and respect. At our school we want everyone to be valued, to explore the joy of learning, and to achieve their full potential.

Introduction

St Mary & St John takes the safety of all the children and adults very seriously. This policy is written to protect all children and adults. We recognize that E-Safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. This E-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others. These risks to E-Safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defense; their observation of behavior is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Scope

This policy applies to all pupils, all staff, all governors and all volunteers.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters. □ Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely

- All pupils will be taught about E-Safety.
- All pupils will be shown an age appropriate E-Safety presentation, which will help them to identify and report any inappropriate content.
- Pupils in Year 5 & 6 will learn about appropriate behavior while using social media.
- Pupils in Year 6 will attend Junior Citizen.

Data Protection

- There is a separate Data Protection policy.

E-mail

- Staff will only use approved e-mail accounts when using the school network.

Internet Access

□ Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

Mobile Phones and other handheld technology

Pupils are not permitted to have mobile phones or other personal handheld technology in school. When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP). Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (*Education and Inspections Act 2006, Sections 90, 91 and 94)*.

Systems Security

□ ICT systems security will be regularly reviewed with support from 123ICT.

Web Filtering

- The school will work with 123ICT to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to an appropriate member of staff.

Communication of the E-Safety policy to pupils

- E-safety rules will be posted in each room where a computer is used.
- Pupils will be informed that internet use will be monitored.
- E-Safety will be included in the curriculum and regularly revisited **Communication of the E-safety policy to staff**
- The E-Safety policy will be given to all new members of staff as part of the staff handbook. They will also be available on the Health & Safety noticeboard, website and on the Safeguarding questions in the staff meeting.
- Staff will be informed that internet use will be monitored.

Communication of the E-Safety policy to Parents/Carers

- The school website will include a list of E-Safety resources and information for parents to access.
- The school will communicate and publicise E-Safety issues to parents through the school newsletter and website.

E-Safety Complaints

- Instances of pupil internet misuse should be reported to the E-Safety co-ordinator.
- Staff will be trained so they are able to deal with E-Safety incidents. They must log incidents reported to them as a cause for concern and if necessary refer the matter to a senior member of staff.
- Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher.

Whole-School Responsibilities for Internet Safety Headteacher

- Responsible for E-Safety issues within the school but may delegate the day-to-day responsibility to the E-Safety co-ordinator.
- Ensure that the E-Safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.

- Ensure that developments at Local Authority level are communicated to the E-Safety co-ordinator.
- Ensure that the Governing Body is informed of E-Safety issues and policies. Ensure that appropriate funding is allocated to support E-Safety activities throughout the school.

E-Safety co-ordinator

The Headteacher has identified Lise Bosher as the E-Safety co-ordinator.

- Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).
- Establish and maintain a school-wide E-Safety programme.
- Establish and maintain a staff professional development programme relating to E-Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body

- Appoint an E-Safety Governor, Rob Green, who will ensure that E-Safety is included as part of the regular review of child protection and health and safety policies.
- Support the Headteacher and/or designated E-Safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.

Network Manager/Technical Support Staff

- Provide a technical infrastructure to support E-Safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school’s network.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school’s network.
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the E-Safety coordinator.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Teaching and Support Staff

- Contribute to the development of E-Safety policies. □ Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of E-Safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include E-Safety regularly in the curriculum.
- Deal with E-Safety issues they become aware of and know when and how to escalate incidents.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area. **Wider School Community**
- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.
- Contribute to the development of E-Safety policies.
- Take responsibility for the security of data.
- Develop an awareness of E-Safety issues, and how they relate to pupils in their care.

- Model good practice in using new and emerging technologies.
- Know when and how to escalate E-Safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

- Discuss E-Safety issues with their children, support the school in its E-Safety approaches and reinforce appropriate behaviors at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behavior online.

Adopted: January 2018

Review date: January 2021