Acceptable Use and 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 Primary School 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. The risks to e-safety and acceptable use 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 defence; their observation of behaviour 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 teaching staff, all support 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 will use existing technologies safely

- Pupils will be taught about e-safety.
- Pupils in Year 6 will be shown an e-safety presentation, which will help them to identify and report any inappropriate content.

- Pupils in Year 6 will learn about appropriate behaviour while using social media.
- Pupils in Year 6 will attend Junior Citizen (where the dangers of meeting someone on the internet are highlighted).

Data Protection

- There is a separate Data Protection policy. This is available on the school website and is annually reviewed.

E-mail

- Pupils and staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail for approved activities.

Internet Access

- Staff will read and sign that they have read the Acceptable Use and E-safety Policy at the start of each school year.
- Parents will be sign posted to the Acceptable Use and E-safety policy on the school website.
- 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. 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)*. Mobile phones and smart watches that belong to children are stored in the school office during the day.

Systems Security

- ICT systems security will be regularly reviewed with support from 123ICT (dedicated technician in school every week).

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 Acceptable User and E-safety policy to pupils

- Pupils will be made aware of the Acceptable Use and E-safety policy through the E-safety Code which is displayed in every classroom.
- 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 Acceptable Use and E-safety policy will be given to all staff at the start of each school year.
- Staff will sign that they have read and understood the Acceptable Use and E-safety policy once a year.

Communication of the e-safety policy to Parents/Carers

- The Acceptable Use and E-safety policy will be available on the school website.
- 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 newsletters and the school website.

E-safety Complaints

- Instances of pupil internet misuse should be reported to a member of staff.

- Staff will be trained so they are able to identify and deal with e-safety incidents. They must log incidents on CPOMS (Child Protection Management System) report them to the E-safety Coordinator or Headteacher.
- Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher. If it is the Headteacher, please report to the Chair of Governors (contact details at school office).
- Pupils and parents will be informed of internet misuse.

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 Chris Chamier-Williams as the E-safety Co-ordinator.

- Primary responsibility: establish and maintain a safe ICT learning environment.
- Establish and maintain a school-wide e-safety programme.
- Review Acceptable Use and E-safety policy and procedures.
- Respond to Acceptable Use and E-safety policy breaches in an appropriate and consistent manner.
- Establish and maintain staff professional development relating to acceptable use and e-safety.
- Develop a parental awareness of e-safety matters.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body

- Appoint an E-Safety Governor 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.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated E-safety Co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).

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.
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the E-safety Co-ordinator.
- 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.
- 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, Seesaw or other technologies.
- 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 behaviours 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 a child is conducting risky behaviour online.

Adopted: January 2018

Reviewed: March 2021

Next review: March 2023