

## **Online Safety Policy**

### **Rationale**

In order to provide “a secure setting in which children are encouraged to live the gospel values” in accordance with the school’s Mission Statement, we have developed an Online Safety Policy which highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Online Safety is wide-ranging and encompasses the use of new technologies, internet and electronic communications such as Learning Platforms, mobile phones, Video Conferencing, collaboration tools and personal publishing.

The school has appointed an Online Safety Coordinator, who will liaise with the Designated Child Protection Coordinator as appropriate.

### **Scope**

The Online Safety Policy covers the following areas:

1. Teaching and Learning
2. Managing Internet Access
3. Policy Decisions
4. Communications Policy
5. 4Cs as detailed in KCSIE 2024

### **1. Teaching and learning**

#### **1.1 Why Internet use is important**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

#### **1.2 Internet use will enhance learning**

- The school Internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.
- Pupils will be taught and families advised what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

#### **1.3 Pupils will be taught how to evaluate Internet content**

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Older pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## **2. Managing Internet Access**

### **2.1 Information system security**

- School ICT systems and security will be reviewed regularly.
- Virus protection will be installed on every computer and will be set to update automatically.
- We will seek advice from the Local Authority with regard to technical matters relating to system security

### **2.2 E-mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

### **2.3 Published content and the school Learning Platform**

- The contact details on the Learning Platform should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Members of staff will take overall editorial responsibility for their sections on the school's Learning Platform and ensure that content is accurate and appropriate.
- Parents will take responsibility for monitoring that their children's use of the school Learning Platform is appropriate.
- Whilst the school will make every effort to ensure that content is kept as accurate and correct as possible, it recognises that inaccuracies will occasionally occur. In these circumstances the school will make every effort to correct any errors in as short a time frame as is possible.

### **2.4 Publishing pupil's images and work**

- Photographs may be used with parental permission.
- Pupils' names may be published, however, photographs and names will never appear together.
- Written permission from parents or carers will be obtained before pupils' work is published on the school Learning Platform.

### **2.5 Social networking and personal publishing**

- Through filtering software provided by the LA, the school will block/filter access to social networking sites.
- Through filtering software provided by the LA, newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

## **2.6 Managing filtering and monitoring**

- The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator, who should be known to all members of the school community.
- The Online Safety Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The filtering system blocks access to harmful sites and content.
- The monitoring system identifies when a user accesses or searches for certain types of harmful content on school and college devices

## **2.7 Managing videoconferencing**

- Videoconferencing will be supervised by a member of staff.

## **2.8 Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will not use personal equipment or non school personal electronic accounts when contacting students. They will be issued with a school phone where contact with pupils is required.

## **2.8 Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2018.

# **3. Policy Decisions**

## **3.1 Authorising Internet access**

- All new members of staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- All parents will be asked to agree to and sign a consent form with respect to the 'Online Safety Rules' and the 'Acceptable Use Policy for Parents and Pupils' before being granted Internet access.
- The school will keep a central record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Access to the Internet will be supervised. Lower down the school, pupils will be given access to specific, approved on-line materials.

## **3.2 Assessing risks**

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit regularly ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

## **3.3 Handling Online Safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Where appropriate, advice will be sought from the Police Youth Crime Reduction Officer to understand potentially illegal issues.

## **4. Communications Policy**

### **4.1 Introducing the Online Safety policy to children**

- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

### **4.2 Staff and the Online Safety policy**

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

### **4.3 Enlisting parents' support**

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school Learning Platform.

## **Conclusion**

At St Mary's, we aim to provide a safe environment in which children are relaxed, comfortable and confident. However, in the wider world, children are now able to log on, access media through their phones and play on games consoles and it is no longer possible to keep children isolated from the risks posed by these technologies. As stated in the Cheshire Online Safety policy issued to schools, "We need to ensure that we provide them with the resilience and tools to effectively cope with the 'inappropriate' material or contact that they may become exposed to at some point in their 'on line' lives. This is education for life. We need to teach our children so that they can know what to do and who to talk to keep themselves and others safe".

Reviewed September 2024