



# **E-Safety Policy**

**Implementation date – Sept 2021**  
**Review date – July 2022**

## E-Safety Policy

### **What is E-Safety?**

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It 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.

### **End to End E-Safety**

E-Safety depends on effective practice at a number of levels:

- Responsible ICT/Computing use by all staff and pupils; encouraged by education and made explicit through published policies. This applies to pupil use of their iPads in lessons.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering.

### **Reviewing the E-Safety Policy**

The E-Safety Policy relates to other policies including those for Computing, bullying and for child protection. Phase leaders will act as E-Safety coordinator for their respective phase and will work closely with the Principal and the Designated Safeguarding lead in order to ensure that this policy is followed. The E-Safety Policy and its implementation will be reviewed annually.

### **Teaching and Learning - 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 pupils 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.
- Internet use will enhance learning and is key to the school's effective use of 1:1 iPad technology in classes from Y2 to Y6..
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what online behaviour 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. They will also be taught about appropriate use of electronic devices to share, communicate and upload information, including their own work.
- 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.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

### **Managing Internet Access**

#### *Information system security*

- School ICT/Computing systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the St. Bart's Multi-Academy Trust.

#### *E-mail*

- Pupils may only use approved e-mail accounts/messaging systems on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
- 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 before sending, in the same way as a letter written on school headed paper.

#### *Published content and the school website*

The contact details on the website should be the school address, e-mail and telephone number. Staff names may be published. Staff's or pupils' personal information will not be published.

### *Publishing pupils' images and work*

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school website. This is done on entry to school.
- Pupils' work can be shared securely with their class teacher through the use of Showbie software

### *Social networking and personal publishing*

- The school will block/filter access to social networking sites.
- 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.

### *Managing filtering*

- The school will work with The St. Bart's Multi-Academy Trust, LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, or any internal/external online behaviour that is inappropriate, it must be reported to the phase leader, DSL or Principal.
- The ICT/Computing team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### *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.
- We recognise that there may be valid safeguarding reasons for a pupil to bring their mobile phone in to school (i.e. they may be going to a different destination other than home after school). Following a written request from a parent, pupils in KS2 may be permitted to bring mobile phones to school on the strict condition that they are switched off and handed in to their class teacher to store securely.
- In the event that a mobile phone is brought in to school and is not handed in or is misused, permission for that pupil to bring their phone to school will be suspended.
- Staff must keep their own mobile phones hidden from view during lesson time.
- The sending of abusive or inappropriate text messages is forbidden.
- More information regarding the use of mobile phones is included in the school's 'Protocol for the use of Mobile Phones' document.

### **Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the SBMAT GDPR policy.

### **Policy Decisions**

#### *Authorising internet access*

Access to the internet will be by supervised access to specific, approved on-line materials and applications.

Management of this takes place centrally by the SBMAT ICT team.

#### **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 or tablet. Neither the school nor local authority can accept liability for the material accessed, or any consequences of internet access.

The school will audit ICT/Computing provision to establish if the E-Safety policy is adequate and that its implementation is effective.

#### **Handling E-Safety complaints**

Complaints of internet misuse will be dealt with by a senior member of staff of at least the rank of Assistant Principal. Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be dealt with in accordance with school's child protection/safeguarding procedures.

#### **Community Use of the iInternet**

External organisations using the school's ICT/Computing facilities must adhere to the E-Safety policy.

## **Communicating the E-Safety Policy**

### **Introducing the E-Safety policy to pupils**

E-Safety "rules" will be discussed with the pupils at the start of each half term and wherever appropriate in between. Pupils will be informed that network and internet use will be monitored.

### **Staff and the E-Safety policy**

All staff will be given the School E-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.

### **Enlisting parents' support**

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