E-Safety Policy

Implementation date – March 2024
Review date – March 2027

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 several levels:

- Responsible ICT/Computing use by all staff and pupils; encouraged by education and made explicit through published policies.
- 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. The Lead Safeguarding Person will also act as E-Safety coordinator. 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.
- 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 internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils in Years 3-6 will use individual iPads to enhance learning experiences. Usage will be closely monitored by class teachers.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation.
- 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 school's Senior ICT/Computing Technician and 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 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 completed on iPads will be carefully monitored so that it is uploaded to secure destinations, namely Showbie for teachers to provide feedback on.

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, it must be reported to the Lead Safeguarding Person.
- 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.
- Pupils are not permitted to bring mobile phones to school. On rare occasions this may be permitted for safeguarding reasons following a request from a parent and is a decision made at the principal's discretion.
- If a mobile phone is brought in to school, it will be held in a secure location by the Class Teacher and returned to the child at the end of the school day.
- Staff must keep 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.

Policy Decisions
Authorising internet access
Access to the internet will be by supervised access to specific, approved on-line materials.

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 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.
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 procedures.

Community Use of the internet
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 year and periodically thereafter.
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 are 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.