St James CE Primary Academy

E-Safety Policy
2017-2019

Aims

To ensure all our children are equipped with the skills required to use electronic equipment safely and responsibly within school and as a life skill.

Children interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place children in danger.

E-safety covers issues relating to children in our care and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school.

E-safety includes education on risks and responsibilities and is part of our duty of care which applies to everyone working with children.

Teaching and learning

- The purpose of Internet use at St James is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the schools management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Class Teachers will indicate on planning where they intend to teach children of their responsibilities and opportunities to remind them as part of good practice in teaching and learning with electronic equipment.
- The evaluation of on-line materials is the responsibility of the Class Teacher and will be monitored by the designated co-ordinator.
- Any concerns raised by staff concerning internet sites, mis-use, or inappropriate pop ups should be logged with the designated E-safety

co-ordinator who will follow the appropriate procedures (outlined under paragraph Responding to risks form)

Managing Information Systems

- **All users** must take responsibility for their own network use.
- Workstations are secured against user mistakes and deliberate actions.
- Servers are located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices is pro-actively managed.(School ICT technician)
- All Internet connections are arranged via the Wolverhampton network to ensure compliance with the security policy.
- Firewalls and switches are configured to prevent un-authorised access between schools.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not used without specific permission followed by a virus check.

Managing E-Mail

- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised by a Teacher before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff will use @st-james.staffs.sch.uk domain addresses for school related emails.

How will published content be managed?

Work or images uploaded onto our website will be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, e-mail and telephone number. Staff or children personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The principal and designated co-ordinator for e-safety will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the schools guidelines for publications including respect for intellectual property rights and copyright.
- Images of a pupil should not be published without the parents or carers written permission.
- Images that include children will be selected carefully and will not enable individual children to be clearly identified.

Managing Social networking

- St James will block/filter access to social networking sites.
- Children will be taught never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Children should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Staff and children will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Children will be encouraged to invite known friends only and deny access to others.
- Children will be advised not to publish specific and detailed private thoughts.

- At St James we will be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. Appropriate responses will be followed if such an incident occurs.

Managing Internet authorisation

- The school will maintain a current record of all staff and children who are granted access to the St James electronic communications.
- All staff must read and sign the Staff Information Systems Code of Conduct before using any school ICT resource.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that children will be provided with supervised Internet access

- **How will risks be assessed?**
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?

- **Complaint recorded(Concern Log sheet)**
- **Complaint handed to designated co-ordinator.**
- **Co-ordinator to refer to Principal.**
- **Decision made on appropriate response.**
- **Relevant parties informed of action to be taken.**
- **Action taken and recorded.**
- **Relevant parties informed.**

Community Cohesion

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by children out of school, e.g. social networking sites, and offer appropriate advice.
- Parents and carers will be supported and a partnership approach to e-safety will be encouraged through workshops and relevant information sent home.
- All staff will be given the School e-Safety Policy and its application and importance explained.
- **Staff will be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.**

All adults with a 'duty of care' to children at St James will attend relevant training to ensure they keep up-to date with their own knowledge and awareness of E-Safety issues.