

## **St James' Catholic High School E-Safety Policy**

### **Teaching and learning**

#### **Why the Internet and digital communications are 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 high-quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

#### **Internet use will enhance and extend learning**

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.

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**

Staff should ensure that the use of Internet derived materials 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 system security will be reviewed regularly.

Virus protection will be installed and updated regularly.

Security strategies will be discussed with the Local Authority.

### **E-mail**

At present, only staff have access to email accounts.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The forwarding of chain letters is not permitted.

## **Published content and the school web site**

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

## **Publishing students' images and work**

Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Work can only be published with the permission of the pupil and parents/carers.

## **Social networking and personal publishing**

The school will control access to social networking sites, and consider how to educate pupils in their safe use.

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, their friends or their location.

Pupils should not place personal photos on any social network space without considering how the photo could be used now or in the future.

Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

## **Managing filtering**

The school will work in partnership with Stockport LA and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to a teacher or the Network Manager.

## **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.

The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

This is one of the reasons why students are not allowed to have mobile phones in school; accordingly mobile phones will not be used during lessons or formal school time and the sending of abusive or inappropriate text messages is forbidden.

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

A school phone will be issued to staff where contact with students is required e.g. during school trips.

### **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**

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Pupils must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy

Parents/carers will be asked to sign and return a consent form (within the pupil planner)

### **Assessing risks**

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Stockport LA can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and 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 headteacher.

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.

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

E-Safety rules will be posted in all rooms where computers are used.

Pupils will be informed that network and Internet use will be monitored.

A programme of training in E-Safety will be delivered to all Year 7 pupils during ICT lessons.

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

All staff will be given the School e-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Staff using social networking sites such as 'Facebook' should take the appropriate steps to ensure that personal data is not readily available and ensure that pupils are unable to access personal details. In addition staff must not engage in any interaction, through social networking sites, which compromises the school, their professional standing or puts them in breach of their contract of employment.

### **Enlisting parents' and carers' support**

Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of E-Safety resources for parents/carers.

Approved for use in March 2010  
Review due: July 2012