Sir James Smith's Community School

Aspiration Ambition Achievement

E-SAFETY POLICY

November 2017

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The schools e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Anti-Bullying, Teaching and Learning, Data Protection.

Good Habits

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

- Responsible ICT use by all staff and students; 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 content filtering.
- National Education Network standards and specifications.

E-Safety Policy

~~The school will appoint an e-Safety group. This will be the Deputy Head, Designated Teacher, the Head of Computing and ICT, the Business Manager, e-safety lead and Link Governor.~~

Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and will be approved by governors.

The e-Safety Policy will be reviewed at least annually.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access.

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;

- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DfE

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted Internet access
- All staff and volunteers must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Parents will be informed that students will be provided with supervised Internet access
- Parents will be asked to sign and return a Parent/Carer Acceptable Use Policy form for student access
- Students must sign and agree to the student Acceptable Use Policy

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the class teacher or ICT Technician.
- Sir James Smith School will ensure that the use of Internet derived materials by students and staff complies with copyright law
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Email

- Students will be provided with a school email account which should be used for school business
- Students must immediately tell a teacher if they receive offensive e-mail
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully. The forwarding of chain letters or viral messages is not permitted

Social Networking

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others

Filtering

The school works with Cornwall Council using their guidelines and use Netsweeper internet filtering solution monitored by NCI Technologies.

Video Conferencing

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Video conferencing will be appropriately supervised for the pupils' age

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
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden
- SIMS is the chosen MIS
- Microsoft Exchange is the chosen email system for students
- Netsweeper internet filtering is the current chosen system
- Use of personal devices if appropriate with the consent of the class teacher for teaching and learning purposes in line with BYOD Policy.

Published Content and the School Web Site

- The contact details on the Web site will 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

Publishing Students' Images and Work

- Photographs that include students will be selected carefully and will be appropriate for the context
- Students' full names may be used anywhere on the Web site, Blog or Social Networking
- Written permission from parents or carers will be obtained on entry to the School before photographs, or full names, of students are published on the School Web site or on Social Network
- Work can only be published with the permission of the student and parents

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the school's SLT and Cornwall Council
- There is restricted access to the Schools Server Room

Protecting Personal Data

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

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Cornwall Council can accept liability for the material accessed, or any consequences of Internet access.

~~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 using the 360° degree safe tool.~~

Handling e-safety Complaints

- Complaints of Internet misuse by students will be dealt with by a member of the Extended Leadership Team. Any complaint about staff misuse must be referred to the Deputy 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

Communication of Policy

Students

- Rules for Internet access will be posted in all ICT rooms
- Students will be informed that Internet use will be monitored
- Students will sign an acceptable use policy when they start the School and this will be reviewed annually

Staff

- 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
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues
- All staff will sign an acceptable use policy before having access to the ICT system
- ESafety is a standing item on the Governors' ICT Group Panel

Parents

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school Web site

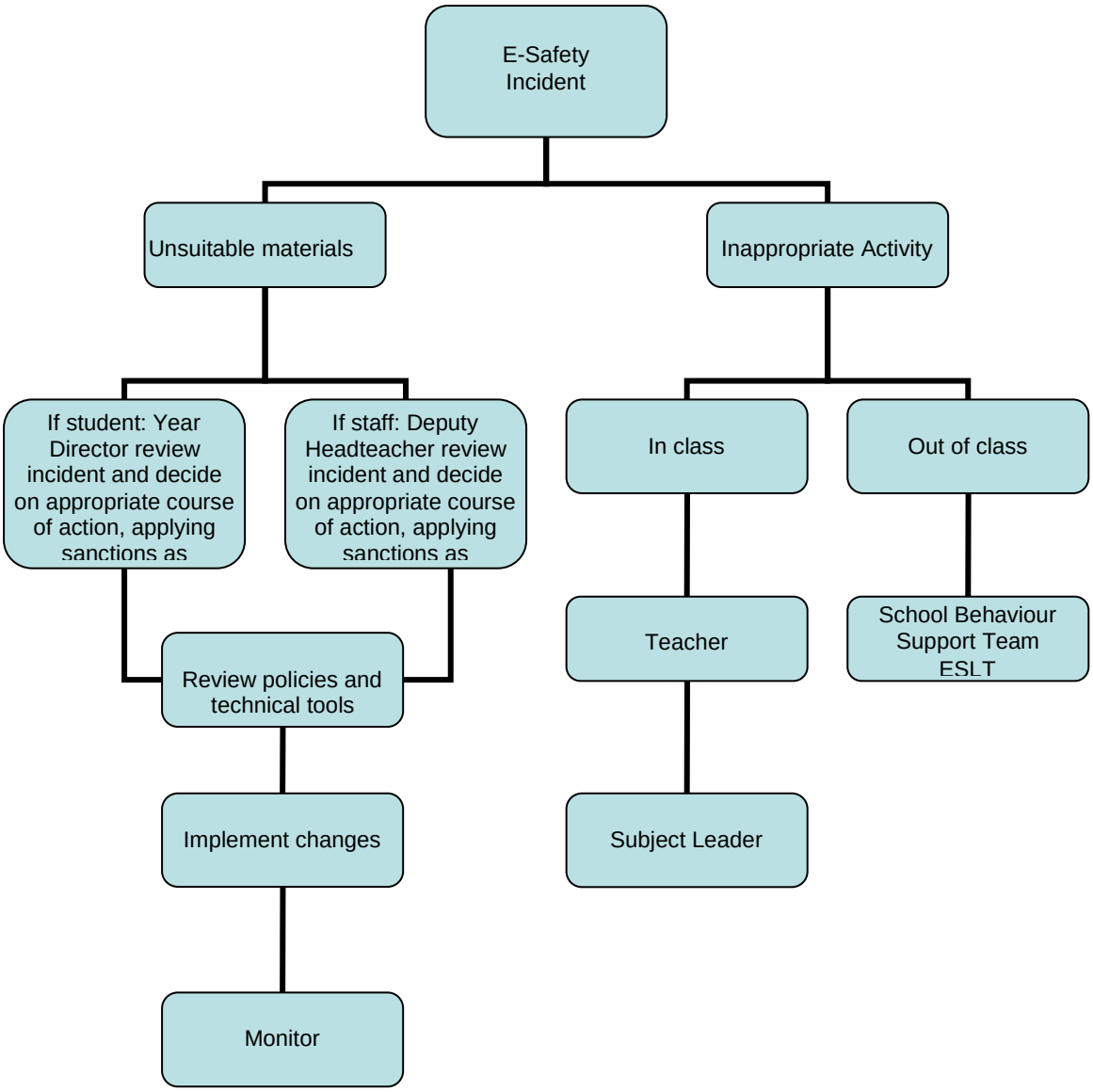
E-Safety Information

The e-safety information can be located on the schools website and is displayed to each user before logging into the system. There is also an E-Safety notice board displayed on the languages corridor in the school.

If you would like this in a different format please contact the school

First Adopted – June 2013
Reviewed by – ICT Panel
Reviewed – November 2017
Ratified by Governors – November 2017
Next Review due – November 2018

E-Safety incident flow Chart



E-Safety Rules

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
  Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to an education establishment.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.