ST VINCENT'S SCHOOL

A Specialist School for Sensory Impairment and Other Needs

Policy Document Title:	E Safety Policy
To be read in conjunction with:	ICT Policy Mobile Phone Policy Staff handbook Internet Access Policy Health and Safety Policy
Updated:	07/12 SR
To be reviewed:	07/12

Rationale

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate our children 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 purpose of Internet use in school is to promote pupil achievement, raise educational standards, 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 an invaluable tool for learning. It is now an essential element in 21st century life and access to the Internet is therefore an entitlement for all pupils who show a responsible and mature approach to its use. Pupils also use the Internet outside of the school and setting and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Policy Links

The school's e-safety policy will operate in conjunction with other policies including Safeguarding Statement, Child Protection / Safeguarding Policy, Health and Safety Policy, Mobile Phone Policy, Code of Conduct, Discipline, Rewards and Sanctions Policy, Anti-Bullying Policy, International links Policy

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

- Responsible ICT 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 for learning including the effective management of content filtering.
- National Education Network standards and specifications.

E-safety considers the following technologies: PCs, laptops, webcams, digital video equipment, mobile phones, portable media players, games consoles and personal digital assistants. All persons either using technology or supervising the use of technology are required to abide by this policy.

E-safety requirements relate to school-owned technology and also to personal technologies

E-safety requirements are applicable during the times whereby the school is opened; this applies to term-time, extended school events, lettings for community use. It is also relevant to residential/off-site events e.g. school trips and visits.

Designated Person for E-Safety Policy

The school will appoint an e-Safety coordinator. The e-Safety Coordinator is Mr S Irvine.
The e-safety Coordinator will be responsible for annual audit. (Appendix C)
Our e-Safety Policy has been agreed by the staff of the school and approved by the governing body.

Internet: The Benefit to Education

Benefits of using the Internet in education include:

- Fully supports the school's implementation and delivery of a creative International Curriculum to enhance learning opportunities
- Access to world-wide educational resources
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils 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
- The school Internet access will be designed expressly for pupil use and includes 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
- Internet access will be planned to enrich and extend learning activities
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- Our school will comply with copyright law
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form for pupil access.

Safeguarding Children and Child Protection

This policy is an extension of the safeguarding children and child protection policies. Caution is expressed to the whole school community as regards child safety in the virtual world as well as the real world. Social networking sites, the uploading of inappropriate web content and cyber-bullying are issues that adults must ensure vigilance and ensure appropriate means are put in place to safeguard and educate our children. It is expected that children who are able, will develop their own protection strategies for when adult supervision and technological protection are not available.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator or network.
- School will ensure that the use of Internet derived materials by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils 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 and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- The schools will filter access to social networking sites and newsgroups 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
- Pupils will be advised not to place personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

Filtering

The school will endeavour to ensure appropriate filtering systems are in place and as effective as possible.

Video Conferencing

- If used videoconferencing 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.(See mobile phone policy)
- Staff will be issued with a school phone where contact with pupils is required.

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 Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified or their image misused.
- Pupils' full names will not be used anywhere on the Web site, 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 will only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

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. The school cannot 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.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff. (Appendix A)
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms. (Appendix B)
- Pupils will be informed that Internet use will be monitored.

Staff

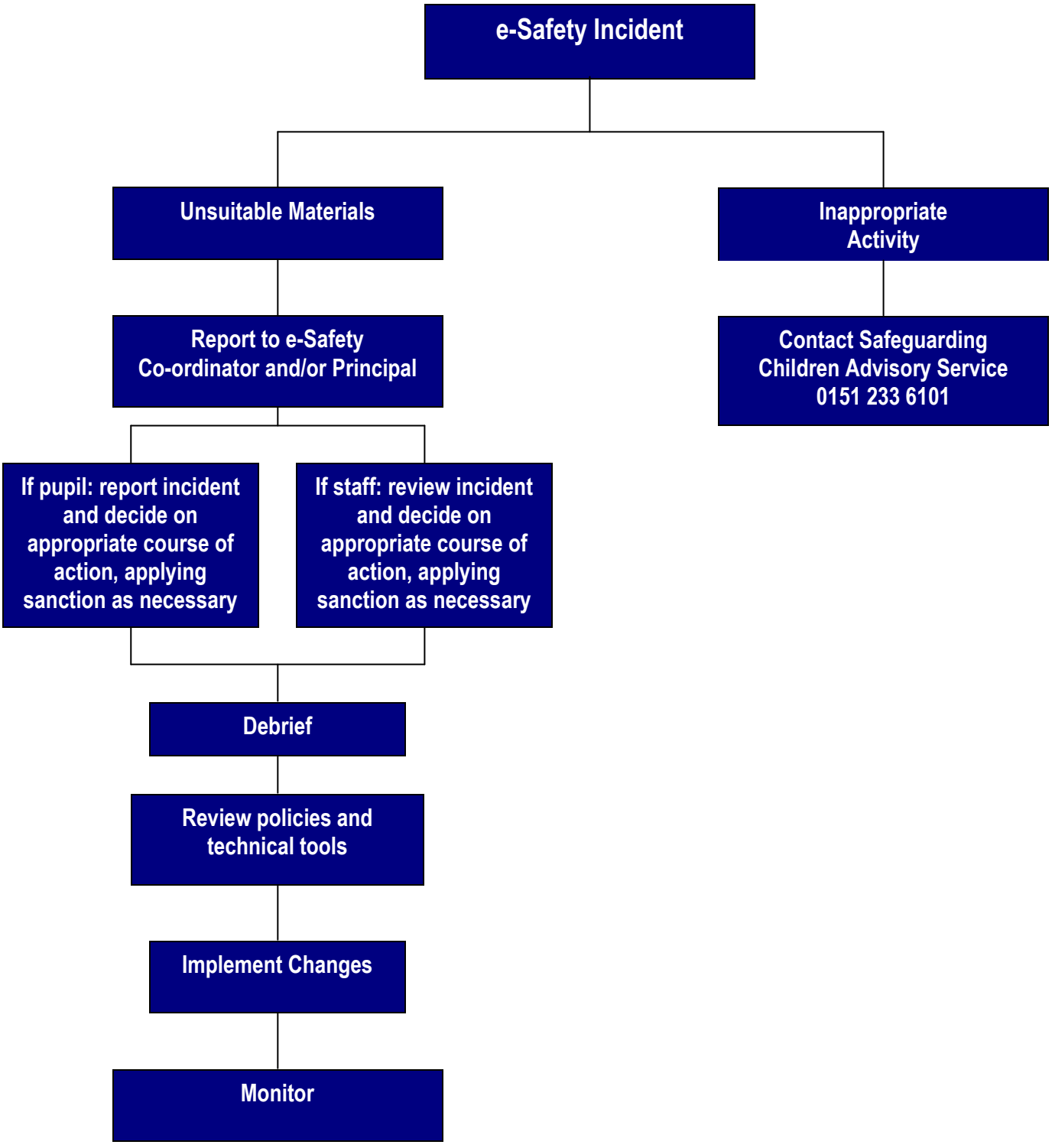
- All staff will be given the School e-Safety Policy and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. (Appendix D)

Parents

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

Referral Process – Appendix A



Appendix B

Key Stage 1 & 2 e-Safety Rules

Think then Click

These rules help us to stay safe on the Internet

- **We only use the Internet when an adult is with us**
- **We can click on the buttons or links when we know what to do**
- **We can the Internet with an adult**
- **We always ask if we get lost on the Internet**
- **We can send and open emails together**
- **We can write polite and friendly emails to people that we know**

Key Stage 3, 4 & Post 16 e-Safety Rules

Think then Click

These rules help us to stay safe on the Internet

- **We ask permission before using the Internet**
- **We only use websites that an adult has chosen**
- **We tell an adult if we see anything that we are uncomfortable with**
- **We immediately close any webpage we are not sure about**
- **We send emails that are polite and friendly**
- **We never give out personal information or passwords**
- **We never arrange to meet anyone we don't know**
- **We do not open emails sent by anyone we don't know**
- **We do not use internet chat rooms**

Appendix B – e-Safety Rules acceptable use

e-Safety Rules

These e-safety rules help to protect pupils 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 reason 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 education.**
- **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.**
- **The school ICT systems may not be used for private purposes, unless the Principal has given specific permission.**
- **Use for personal financial gain, gambling, political activity,**
- **advertising or illegal purposes is not permitted.**

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, 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

Appendix C E-Safety Audit

Good Habits

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

- Responsible ICT 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 content filtering.
- National Education Network standards and specifications.

E-Safety Audit

Has the school an e-Safety Policy that complies with CYPD guidance?	Y
Date of latest update:	March 2012
The Policy was agreed by governors on:	
The Policy is available for staff :	Intranet
And for parents at:	Website
The designated Child Protection Officer is:	J Bradshaw
The e-Safety Coordinator is:	S Irvine
Has e-safety training been provided for both pupils and staff?	Y / N
Do all staff sign an ICT Code of Conduct annually?	Y
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y
Have school e-Safety Rules been set for pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access?	Y
Has the school filtering policy has been approved by SLT?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Appendix 9: Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information:

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Principal
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data (in paper or electronic format) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

Staff have been made aware that breaches of this code of conduct that, for example, result in a child's personal details coming into the public domain, may be investigated by the Information Commissioner and may result in a substantial fine of up to five million pounds.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information 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.

I have read, understood and agree with the information Systems Code of Conduct.

Signed:

Print Name:

Date: