Sharmans Cross
Junior School

e-Safety Policy

Responsibility for e-Safety

The e-Safety Policy provides an important part of schools' safeguarding provision for pupils. Our e-Safety Policy has been written by the school, building on the SMBC Schools e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors and the Parents.

As with all aspects of Child Protection, it is everybody's responsibility to ensure that every reasonable step is taken to keep our children safe at all times. The school has a designated e-Safety Coordinator, who is also the Designated Child Protection Coordinator as the roles overlap.

The e-Safety Policy and its implementation is reviewed each year.

The Internet

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. 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 quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries and to experts in many fields for pupils and staff;
- inclusion in the National Education Network connecting all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 SMBC and DfES;
- access to learning wherever and whenever convenient.

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 will be given clear objectives for

Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff guide pupils in on-line activities that will support the 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.

Rules for Internet access are posted in all networked rooms. Pupils are informed that Internet use will be monitored.

All staff have access to the School e-Safety Policy and its importance is explained. Staff are 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 are supervised by senior management and have clear procedures for reporting issues. Staff development in safe and responsible Internet use and on the school e-Safety Policy is provided as required.

Parents' attention is drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site. A partnership approach with parents is encouraged including parents' evenings with demonstrations and suggestions for safe home Internet use. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet are regularly made available to parents.

The school maintains a current record of all staff and pupils who are granted Internet access. All users read and sign the 'Acceptable ICT Use Policy' before using any school ICT resource. Parents are informed that pupils are provided with supervised Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. The Head Teacher and Governing Body ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Evaluating Content

The school ensures that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. If staff or pupils discover unsuitable sites, the URL (address), time, date and content is reported to Solihull ICT Services, and where appropriate the school e-safety officer. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. The evaluation of on-line materials is a part of every subject.

Published Content

The only contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate. The Web site respects intellectual property rights and copyright.

Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified. Pupils' full names are not used anywhere on the Web site, particularly in association with photographs. Written permission from parents or carers is obtained before photographs of pupils are published on the school Web site. Pupils' work can only be published with the permission of the pupil and parents. Images of staff are not published without consent.

Social Networking

Social networking sites can connect people with others for a wide range of purposes, including educational purposes. Guests can be invited to view personal space, pupils' work or documents and leave comments. There is increasing educational use of such tools, for example in the use of blogs and wikis to improve writing. Social networking has many possibilities for staff and pupils working together and is increasingly used in an educational context.

Social networking sites and newsgroups are blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location. Pupils are advised not to place personal photos on any social network space. Advice is given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.

Teachers' official blogs or wikis are password protected and run from the school website. Teachers must not run social network spaces for students on a personal basis. Teachers must not communicate with pupils through private social networking sites, even on educational matters, but should use official sites sanctioned by the school.

Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others. They are advised not to publish specific and detailed private thoughts.

We are 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.

Managing Filtering

The school works in partnership with the Solihull MBC and Becta to ensure filtering systems are as effective as possible. If staff or pupils discover unsuitable sites, the URL, time and date are reported to the school E-Safety coordinator. Senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal is reported to the appropriate agencies such as IWF or CEOP.

Managing Emails

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. Use of words included in the filtering/checking 'banned' list are detected and logged. The forwarding of chain letters is not permitted.

Video Conferencing

Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. Adults establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. IP videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet. Equipment connected to the educational broadband network uses the national E.164 numbering system and displays their H.323 ID name. External IP addresses are not be made available to other sites. Videoconferencing contact information is not put on the school web site.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing is supervised. Parents and guardians must agree for their children to take part in videoconferences. Unique log on and password details for the educational videoconferencing services are only be issued to members of staff and kept secure.

If recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely. If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology, and effective practice in classroom use should be developed. The safest approach is to deny or severely control and restrict access until a risk assessment has been completed and safety demonstrated.

Virtual classrooms and virtual communities widen the geographical boundaries of learning. New requirements for online reporting to parents are being introduced. On-line communities may encourage a disaffected pupil to keep in touch or provide access to learning for an isolated pupil. The safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites. The registering of individuals to establish and maintain validated electronic identities is an important part of the process.

Managing Information Services

The security of the school information systems aree reviewed regularly. Virus protection is updated regularly. Security strategies follow Solihull MBC guidelines. Personal data sent over the Internet is encrypted or otherwise secured. Portable media may not used without specific permission followed by a virus check. Where they are used to store personal information they are encrypted. Unapproved system utilities and executable files are not allowed in pupils' work areas or attached to e-mail. Files held on the school's network arebe regularly checked. The ICT co-ordinator / network manager reviews system capacity regularly.

Protecting Personal data

The quantity and variety of data held on pupils, families and on staff is expanding quite quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to

protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual).

The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individuals rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

Personal data is recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998.

e-Safety Complaints

Formal complaints of Internet misuse are dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the head teacher who should use the agreed SMBC procedures. Pupils and parents are informed of the complaints procedure. Sanctions for pupils within the school discipline policy include: interview/counselling by head of year or senior leader; informing parents or carers; removal of Internet or computer access for a period.

Community Links

The Internet is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. Ideally, young people would encounter a consistent policy to Internet use wherever they are.

In community Internet access there is a fine balance to be achieved in ensuring 'freedom of information' whilst providing adequate protection for children and others who may be offended by inappropriate material. We will liaise with local organisations to establish a common approach to e-safety.

Date: January 2011
Review: January 2012