

RATIONALE

The e-Safety Policy relates to other policies including those for bullying and for child protection. The SLT member responsible for IT is also the second designated Child Protection Officer.

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 students.

AIMS

This policy aims to raise awareness on how we can embrace new technologies whilst educating students and staff on how to stay safe.

KEY PRINCIPLES

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, evaluation and personal safety online.
- We endeavour to ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting it's accuracy.
- 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 SCC can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

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.
- Securus is used to monitor system activity.

E-MAIL

- Students are provided with e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. The student e-mail system does not accept external emails
- The school should consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted and limits are in place to prevent these.

PUBLISHED CONTENT/SCHOOL WEB SITE

- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
- Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused.
- Work or photographs can only be published with the permission of the student and parents/carers. They have the option to refuse permission when completing induction paperwork. Students are expected to inform relevant staff if their work or image is not to be published, at the time.

SOCIAL NETWORKING

- The school will control access to social networking sites, and consider how to educate students in their safe use. They are currently blocked through the County filtering system.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students 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.

FILTERING

- The school will work in partnership with SCC, SWGfL, Becta and the Internet Service Provider to ensure that systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to their IT teacher, the e-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

VIDEO CONFERENCING

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

EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Senior staff should note that technologies such as mobile phones with alternative access to the internet, can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not normally be used during lessons or formal school time (unless the particular lesson or aspect of the curriculum requires it). The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones to capture their own work, will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access. Care is required in any use in school.

PROTECTING PERSONAL DATA

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

AUTHORISING ACCESS

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents/carers will be asked to sign and return a consent form.

e-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by the Headteacher, e-safety coordinator or Subject Leader for IT.
- 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 safeguarding procedures.
- Complaints about e-bullying must be dealt with in accordance with school anti-bullying policy.

COMMUNICATING e-SAFETY

- e-Safety rules will be posted in all rooms where computers are used and on the school website.
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety is delivered, based on the materials from CEOP.
- 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 staff and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship. Communicating with students via social networking sites is advised against.
- 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 e-Safety Policy is reviewed by SLT, Subject Leader for IT and the Network Manager on an annual basis and submitted to the Governing Body for approval.

Reviewed and updated September 2009