



Elmhurst School

E-Safety

by

Darren J. Bisbey Bsc (Hons), AIOSH

October 2010

Overview

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The AUP (Acceptable User Policy) policy will be reviewed on an annual basis to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The Elmhurst E-Safety Policy has been written by the I.T Manager who has followed government advice and guidance.

The school's E-Safety policy will operate in conjunction with other policies including those for I.C.T, Student Behaviour, Bullying, Curriculum, Safeguarding Children, Data Protection and Security.

The school will appoint an E-Safety Coordinator. This may be the Designated Safeguarding Children Coordinator as the roles overlap.

Teaching and Learning

Why Internet use is 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 quality Internet access as part of their learning experience.

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

Students 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.

Internet use will enhance learning

The school Internet access will be designed expressly for student & staff use and will include filtering appropriate to the school policy.

Students will be taught appropriate use of the Internet.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.

Staff should guide students in on-line activities that will support the 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.

Students will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and 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 its accuracy.

Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with SLICT (Strategic Leadership in ICT) group.

E-mail

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation 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.

Published content and the school Website

The contact details on the Website should be the school address, e-mail and telephone number. Staff or Students' personal information will not be published.

Publishing student's images and work

- Photographs that include students will be selected carefully.
- Students' full names will not be used anywhere on the Website or Blog in association with photographs.
- Written permission from parents or carers is obtained on entry to the school. Please refer to the 'Using Photographic Images of Children' consent form.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- 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 or their location.
- ***N.B. the School is in the process of developing a 'Social Networking' Policy.***

Managing filtering

The SLICT Group will monitor & discuss the requirement for students requests to access banned websites.

If staff or students discover an unsuitable site, it must be reported to the E-Safety Coordinator.

The SLICT group will 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 must be reported to appropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child Exploitation and Online Protection).

Managing video conferencing

Video conferencing (Skype etc.) will be reviewed and discussed by the SLICT group.

Students should ask permission from the supervising teacher before making or answering a videoconference call.

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 are not permitted in the school building (students in the Sixth Form are exempt as per the School Rules) and must not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

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

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.

It is an assumption that ALL staff & students have internet access, provided by Elmhurst.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

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 Principal.

Complaints of a Safeguarding Children nature must be dealt with in accordance with school Safeguarding Children procedures.

Parents and students will need to work in partnership with staff to resolve issues.

Communications Policy

Introducing the E-Safety policy to Students

E-Safety rules will be posted in all networked rooms with Internet access and discussed with the Students at the start of each year.

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

Staff and the E-Safety policy

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 training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy in newsletters, and on the School Website.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Written October 2010

To be reviewed October 2011