



Slough and Eton Church of England Business and Enterprise College



*A Member of Slough and East Berkshire C of E
Multi Academy Trust*

e-Safety Policy

Owner:	Mr Martin Culkeen
Ratified by Governing Body:	<i>James MB Scragg</i>
Date Ratified:	20/02/2018
Date Policy to be reviewed:	Autumn 2018



Contents

Teaching and Learning.....	Page 1
Managing Internet Access.....	Page 2
Policy Decisions.....	Page 3
Communications Policy.....	Page 4
Misuse.....	Page 4



e-Safety encompasses internet technologies and electronic communications such as mobile/smart phones, iPads and tablets. 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.

This e-Safety Policy

- reflects the need to raise awareness of the safety issues associated with electronic communications as a whole
- will operate in conjunction with other school policies including those for ICT, Behaviour, Child Protection, Curriculum Planning, and Health & Safety
- has been written by the school, based on a template provided by Slough Borough Council which itself is based on government guidance and is considered a model of good practice nationally

Further information can be found at:

<http://www.becta.org.uk/schools/esafety>

<http://www.ceop.gov.uk/>

Slough and Eton operates a structure where a Deputy Headteacher line manages whole school ICT and the ICT working party and is thus the e-Safety Coordinator. This role is enhanced by the designated Child Protection Coordinator as the roles overlap.

This e-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why is use of the Internet so 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.

What are the benefits of using the Internet for the education of our children?

- 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
- staff professional development through access to national developments, educational materials and good curriculum practice
- communication with support services, professional organisations and colleagues
- improved access to technical support including remote management of networks and
- exchange of curriculum and administrative data at both local and national government levels

How will Internet use enhance the learning of students?

- The school Internet access will be designed expressly for student use and will include appropriate filtering



- Students will be taught what Internet use is acceptable and what is not and be given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will students be taught 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 it's accuracy.

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 the Local Authority.

E-mail

- Students may only use approved e-mail accounts on the school system.
- Students may not access social networking sites except when authorised to do so for educational purposes.
- Students must immediately tell a teacher if they receive an offensive e-mail or emails
- Students must not reveal personal details of themselves or others in e-mail communications, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully 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.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. In practice monitoring may be delegated to appropriate members of staff.

Publishing student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified by name.
- Students' full names will not be used anywhere on the Website or Blog, particularly in association with photographs.
- As part of the admissions procedure parents are asked to grant permission for photographs of students to be taken and to be used in promoting the school. If parents wish to withdraw their child at any time they are asked to put this in writing.



Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students, parents and staff will be advised about the risks of using social network spaces outside school.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved as necessary.
- If staff or students discover an unsuitable site, it must be reported to the ICT Helpdesk or e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Where necessary sites will be reported to CEOP and CEOP guidance followed.

Managing videoconferencing

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' 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 only be used in accordance with school policy. The sending of abusive or inappropriate text messages, or similar, 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 the 'Electronic Information and Communications Policy' before using any school ICT resource.
- The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- As part of the admissions procedure parents are asked to grant permission for their son/daughter to use the Internet. If parents wish to withdraw their child at any time they are asked to put this in writing.



Assessing risks

- In common with other media such as magazines, books, videos and DVDs, some material available via the Internet is unsuitable for our students. 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. Neither the school nor Slough Borough Council 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.

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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-Safety.

Communications Policy

Introducing the e-Safety policy to students

- E-safety rules will be posted in all networked rooms 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

- At induction, all staff are made aware of 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.

Enlisting parents' support

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

Misuse

Misuse of the internet in school, or affecting school, will result in students being dealt with under the School Behaviour Policy or for staff under the Staff Disciplinary Policy.