Pol35– E-Safety Policy

Objectives

We at **Olive Secondary School** aim to provide all pupils full access to all aspects of school life.

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 pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Relevant Legislation

In this connection, related (e-safety) legislation is as follows:

- Section 146 (April 2005) of the Criminal Justice Act 2003
- The Children's Act 1989
- Sexual Offences Act 2003
- Racial and Religious Hatred Act 2006

The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour Management, Bullying, Teaching & Learning and Data Protection. See Pol 3- child protection and safeguarding policy for further information. 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 Network including the effective management of K9 filtering.

Pol35– E-Safety Policy

SCHOOL

National Education Network Standards and Specifications

Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

End to End E-Safety

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

- Responsible ICT use by all staff and students; 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 network including the effective management of filtering.

Writing and Reviewing the E-Safety Policy

- The e-Safety Policy is part of the School Development Plan and relates to Including those for ICT, bullying and for child protection.
- The school's e-safety policy will be written by the e-safety board and agreed by the head teacher.
- The current e-Safety Policy has been written by the school and may be amended from time to time to make it more effective.
- It has been agreed by senior management, the e-safety board and approved by the Head Teacher.
- The e-Safety Policy and its implementation will be reviewed annually.

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 pupils.

Pol35– E-Safety Policy

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 given clear objectives for Internet use.

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

Pupils will be taught how to evaluate Internet content

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an 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.
- E-mail sent to an external organization should be written carefully and authorized 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 Web Site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work

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

Social Networking and Personal Publishing

- School will block/filter access to social networking sites and their use is not permitted on any of the school's ICT resources.
- Newsgroups will be blocked 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 must not place personal photos on any social network space.
- Should pupils use social network sites in their own homes they will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.
- Students should be encouraged to invite known friends only and deny access to others.

Managing Filtering

- The school will work in partnership with the Internet Service Provider to ensure systems are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the concerned staff.
- All social networking sites and media sites shall be blocked using K9 filtering software or any other such program advised by school senior management.

Network Management

Senior staff will ensure that regular checks are made to ensure that the Filtering methods selected are appropriate, effective and reasonable.

Managing Videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- 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 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

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- All the staff members and student must sign the Internet Access Document titled as Responsible Internet Use.
- All students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents will be asked to sign and return a consent form.

- All staff should be using only the school dedicated email address on the school hosting server for all official and school related correspondence.

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 should 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.
- A help email will be provided at the school hosting server / website in case of any need by a student or staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the local Police to establish procedures for handling potentially illegal issues.

Community Use of the Internet

The school may liaise with local organizations to establish a common approach to e-safety if the need arises.

Communications Policy

Introducing the E-Safety Policy to Pupils

- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.

- Create awareness among all year groups of how to use internet safely.
- Hold assemblies, quizzes, sessions and other such activities to create awareness among the students about e-safety.
- Appropriate age-related curriculum should be developed for creating awareness among the students.

Staff and the E-Safety Policy

- All staff will be given the School e-Safety Policy and its importance explained.
  - The E-Safety board meets termly, including the headteacher, the ICT teacher and middle manager.
  - Staff should be 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 will be supervised by senior management and have clear procedures for reporting issues.
  - The yearly plan shall include systematic training and awareness sessions for the staff. Training sessions shall be arranged during non-contact days or during term time, if necessary.
  - It is compulsory for all staff including non-teaching staff to attend all the training sessions.
  - All staff including non-teaching staff is required to fully comply with the policy and implement it as and whenever the situation arises.

Complying to Ofsted Training Requirements

The school will make every attempt to provide training to staff, students and parents on the areas indicated in the Ofsted guidance, January 2014. The following three areas will specially focused on during e-safety training sessions.

Content

- Exposure to in-appropriate content such as:

- Online pornography

- Ignoring age rating in games

- Substance abuse
- Life style websites such as self-harm, pro-anorexia, suicide sites , hate sites etc.
- Content Validation

Conduct

- Grooming
- Cyber-bullying
- Identity theft, phishing including (hacking fraping i.e. Facebook profiles) and sharing passwords

Contact

- Privacy issues, including disclosure of personal information.
- Digital footprints and online reputation
- Health and well-being (amount of time spent online such as internet and gaming)
- Sexting
- Copyright

Enlisting Parents' Support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site. The school shall work closely with the parents to continue the e-safety support at home.

Reviews and Revisions

This policy shall be reviewed from time to time for revision purposes. Any unnecessary details may be deleted or more relevant details may be added if necessary. The policy may be amended at any time and approved by the head teacher.

Each year, a fully updated version of the policy shall be published when the expiry of the Policy.

Appendix -1
Internet Access Document

Responsible Internet Use

The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Users must access the Internet only via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's educational programme of study.
- Copyright and intellectual property rights must be respected.
- Users are responsible for the e-mails they send and for contacts made.
- E-mails should be written carefully and politely. As messages may be forwarded to unintended readers, e-mail is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms is not allowed.

- The school ICT systems may not be used for private purposes, unless appropriate authorisation has been given.

- Use for personal financial gain, gambling, advertising or any activity which the school deems offensive is forbidden.

- The security of ICT systems must not be compromised.

- Laptops used on the school premises may only connect to the internet via the school's network and internet filtering service.

- The downloading and exchanging of illegal music files across the school network is not allowed.

- The school cannot be held responsible for Internet content accessed using devices other than school computers and laptops. e.g 3G/4G mobile phones, Tablets etc

- Irresponsible use may result in the loss of network or Internet access.

The school will exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Those responsible for the unauthorised use of the school's computers will be subject to the full disciplinary sanctions available to the Head teacher and senior management.