E-Safety Policy

Introduction

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.

The school's e-safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying and Curriculum

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.
- Safe and secure broadband including the effective management of filtering systems.

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.

Internet use will enhance learning

- 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them 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

- Staff 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

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

Published content and the school website:

- 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 Directors 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, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- Social networking sites and newsgroups will be 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. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for pupils.

Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible

Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use is allowed in school.
- Mobile phone should 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.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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.
- All Staff are familiar with the PREVENT agenda 2015, school takes its responsibilities very seriously in order to ensure that young people in our care are not at risk of radicalisation.

● The Head Teacher will ensure that the e-Safety Policy is implemented.

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 head teacher.
● 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 be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Updated: September 2016

Reviewed: September 2018

Next review: September 2019