

INTERNET AND E-SAFETY POLICY

E-safety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. 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 experiences.

Why Internet use is important

The Internet is part of everyday life for education, business and social interaction. The school offers provision to pupils to access the internet as part of their learning experience. It is also a resource for both staff and pupils.

Safeguards

- The school internet is protected by a filtering system.
- Pupils will be overseen by staff and will not have unsupervised access to the internet.
- Staff will discuss objectives for internet use and teach pupils about internet safety.
- Pupils will be taught effective use of the internet when researching material including skills in locating, retrieving and evaluating information.
- Staff should ensure that the use of Internet derived materials complies with copyright law.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
-

E-mail

- Pupils may be taught how to e-mail as part of planned curriculum activities.
- Pupils will also be taught about the safe use of e-mails.

Publishing

Published content and the school website

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- Staff or pupils' personal information will not be published.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

Publishing pupils' images and work

- Written permission will be obtained from parent/carers before using any images of a pupil.
- Pupils' full names will not be used anywhere particularly in association with photographs.

Social networking and personal publishing

- School will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must know not to place personal photos on any social network site.
- Pupils should 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, checking with an adult first and deny access to others.

Managing filtering

The school will work with the L.A. to ensure systems are in place and are reviewed to protect pupils. If staff or pupils discover an unsuitable site, it must be reported to the ICT Network Manager. The ICT Network manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

New technologies will be examined for educational benefits and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used during lessons, unless it is shown to be part of the ICT curriculum. For security reasons, pupils who bring mobiles into school (for example independent travellers) need to have a permission letter, and hand their mobile into the school office at the beginning of the day.

Protecting personal data

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

Authorising Internet Access and use of ICT equipment

ICT facilities at the school are provided for the purposes of education and therefore must be used responsibly. Use of ICT facilities must be sensible, lawful, and respectful of the school, its students and staff.

The 'Acceptable Use Agreement' MUST BE read and signed by staff, pupils, parent/carers and community users. Secondary pupils must sign for Internet access and primary pupils where appropriate. An 'Acceptable Use Agreement' will be provided for temporary or supply staff and visitors to the school. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. Due to the international scale of the internet and the fact that it is impossible to guarantee that unsuitable materials will never appear on the school computer, neither the school nor the Governors can accept liability for the material accessed.

The school will audit ICT provision to establish if the e-safety policy is adequate and its implementation is effective.

E-safety complaints

Complaints of a Child Protection nature must be dealt with in accordance with school Child Protection procedures.

Any complaint about staff misuse must be referred to the head teacher.

Introducing the E-Safety Policy

Pupils and the E-safety Policy

E-safety rules will be posted in all networked areas and discussed with the pupils at the start of each year. The importance of e-safety will be taught explicitly as part of our ICT curriculum and will be planned in accordance to the age and maturity of understanding of the children.

Staff and the E-safety Policy

All staff will be able to access the school e-safety policy and its importance explained. Staff should be aware that all 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.

Parental support

Parent/Carers attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school Web site.

Please read in conjunction with all other safeguarding policies.

This policy was reviewed by Governors: 2012