SCHOOL E SAFETY POLICY

1 Writing and Reviewing the e-Safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection.
Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.

2 Teaching and Learning

2. 1 Why the Internet and Digital Communications are Important

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide pupils with high-quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

2.2 Internet Use Will Enhance and Extend Learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Clear boundaries are set for the appropriate use of the Internet and digital communications and published in staff and pupil planners.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.3 Pupils Will Be Taught How to Evaluate Internet Content

- Users should be aware that the use of Internet derived materials by staff and by pupils must comply with copyright law.
- Pupils should be taught to be critically aware of the materials they read and consider the source of information before accepting its accuracy.

3 Managing Internet Access

3.1 Information System Security

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

3.2 E-mail

- Pupils will be provided with approved Lancashire e-mail accounts to be used on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

3.3 Published Content and the School Web Site

- Staff or pupil personal contact information will not generally be published. The contact details given online will be the school office.
- The Headteacher or Network Manager will take overall editorial responsibility and ensure that published content is accurate and appropriate.

3.4 Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully so that vulnerable pupils cannot be identified or their image misused.
- Pupils' full names will not be used on the school Web site or other on-line space, particularly in association with photographs, unless express permission has been given by parents/carers.
- Permission from parents or carers will be obtained through the Contact Details form, issued annually, before photographs of pupils are published on the school Web site.

3.5 Social Networking and Personal Publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

3.6 Managing Filtering

- The school will work in partnership with CLEO and the Westfield Centre to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Network Manager.

3.7 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.
- The senior leadership team must be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Smartphones and games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

3.8 Protecting Personal Data

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

4 Policy Decisions

4.1 Authorising Internet Access

- All staff must read the 'Staff Code of Conduct for ICT', before using any school ICT resource .
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Pupils' Internet access is dependent on their agreement to comply with the Responsible Internet Use statement.

4.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.3 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.
- Pupils and parents will be informed of the complaints procedure.

5 Communicating e-Safety

5.1 Introducing the e-Safety Policy to Pupils

- e-Safety rules will be posted on the school website.
- Pupils will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed through Key Stage 3 ICT lessons.

5.2 Staff and the e-Safety Policy

- All staff will have access to the School e-Safety Policy.
- Staff must be aware that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

5.3 Enlisting Parents' and Carers' Support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.