E- Safety Policy

Overleigh St Mary's CE Primary School

Signed: Janet Davies

Signed: Emma Drew

E-Safety Policy

E-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.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Child Protection, Curriculum, Data Protection and Security.

Good Habits

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 from the provider including the effective management of content filtering.

- National Education Network standards and specifications.

Dangers to consider

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this.

E-Safety Audit –

This quick self-audit has helped our senior leadership team (SLT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y
Date of latest update: November 20th 2017	
The Policy was agreed by governors: TBC	
The Policy is available for staff at: School Network (Staff Share)	
And for parents at: School Website on E safety section	
The designated Child Protection Teacher/Officer is: Headteacher: Emma Drew	
The e-Safety Coordinator is: Susanna Dixon	
Has e-safety training been provided for both pupils and staff?	Y
Do all staff sign an Esafety code of conduct? TBA	
Is the Think U Know training being considered?(assemblies workshops Nov '17)	Y
Have school e-Safety Rules been set for pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	**Y**
Has the school filtering policy been approved by the SLT?	Y

The school will monitor the impact of the policy using:
- Logs of reported incidents
- broadband monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
- pupils
- parents / carers
- staff

School e-Safety Policy

The school will appoint an e-Safety coordinator. This is currently Susanna Dixon

Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed November 2018

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Many pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates:
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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 learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Parents will be informed that pupils will be provided with supervised Internet access.
- Pupils will be asked to sign the 'Acceptable ICT Use Agreement/ charter' which will also each year which will be displayed in classrooms and in the computing suite.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator or network manager who will investigate and take appropriate action, liaising with broadband provider if necessary
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Social Networking

- School will block/filter access to social networking sites and newsgroups 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 should be advised not to place personal photos on any social network space
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others
- Pupils and parents should be made aware that some social networks are not appropriate for children of primary school age

Filtering

The school will work in partnership with internet Service Provider to ensure filtering systems are as effective as possible.

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden

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 Pupils' Images and Work

- Photographs that include pupils will be selected carefully and relevant information will be considered during the process
- 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

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with our technical support team and broadband provider if necessary

Protecting Personal Data

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

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
- 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 Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

Communication of Policy

Pupils

- Rules for Internet access will be posted in all rooms
- Pupils will be informed that Internet use will be monitored

Staff

- All staff will be given 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.

Parents

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