Offham Primary School

Online Safety Policy

Date of Policy March 2017

Review Date March 2018

Signed – Chair of Governors

Signed – Head Teacher

Online 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.
Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance. It has been agreed by the staff and approved by governors. The e-safety co-ordinator is Mrs Emily John (DCPC).

Why is Internet use important?
Internet use is part of the statutory curriculum and a necessary tool for learning.

The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience.

Pupils use the Internet widely outside school and 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 experts in many fields for pupils and staff.
- Access to world-wide educational resources including museums and art galleries.
- Access to learning wherever and whenever convenient.
- Exchange of curriculum and administration data with KCC and DCSF.

How can Internet use enhance learning?
The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

How will pupils learn how to evaluate Internet content?
Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
The evaluation of on-line materials is a part of teaching/learning in every subject.

How will information systems security be maintained?
The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.
Files held on the school's network will be regularly checked.

Online Safety Policy

How will e-mail be managed?

Pupils may only use approved e-mail accounts. Pupils must immediately tell a teacher if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from a responsible adult.
Whole class or group email addresses will be used for communication outside of the school.
Access in school to external personal e-mail accounts may be blocked.

How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils’ personal information must not be published.

Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace ‘@’ with ‘AT’).

Can pupil’s images or work be published?

Images that include pupils will be selected carefully and will not provide material that could be reused.
Pupils full names will not be used anywhere on the website, particularly in association with photographs.
Written permission from parents or carers should be obtained before images of pupils are electronically published.

How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.

Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

How will filtering be managed?

The school will work with outside agencies to ensure that systems to protect pupils are reviewed and improved.
If staff or pupils discover unsuitable sites, the URL must be reported to the Offham e–Safety Coordinator.
The School’s broadband access will include filtering appropriate to use age and maturity of pupils.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Photographs of Pupils

All staff may only take pictures of pupils on their school cameras. They may not use personal cameras or mobile phones. All pictures are stored on the Offham network only accessed by staff.

How will videoconferencing be managed?

The equipment and network
All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Users
Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing should be supervised appropriately for the pupil's age. Parents and carers must agree for their children to take part in videoconferences.

How can emerging technologies be managed?

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

Staff only use a school phone when contacting parents. Staff would not contact a pupil directly.

How should personal data be protected?

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

How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must read and sign the 'Staff Information Systems Code of Conduct' or Acceptable Use Policy before using any school ICT resource.

Parents will be informed that pupils will be provided with supervised Internet access. They will be asked to sign and return a consent form for pupil access.

At Key Stage One access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

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.

Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?
Complaints of Internet misuse will be dealt with under the School's Complaints Procedure. Any complaint about staff misuse must be referred to the E-Safety Coordinator or Head Teacher.
All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

How is the Internet used across the community?
The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyber bullying be managed?
Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
There will be clear procedures in place to support anyone affected by Cyber bullying.
All incidents of cyber bullying reported to the school will be recorded.

How the school shared area, KLZ, is managed
The SLT will monitor any usage of KLZ, in particular message and communication tools and publishing facilities.

Staff will be advised on acceptable conduct and use when using KLZ.

Only members of the current staff community will have access to the KLZ.

All users will be mindful of copyright issues and will only upload appropriate content onto the KLZ.

When staff leave the school their account or rights to specific, school areas will be disabled.

How will the policy be introduced to pupils?
An e–Safety module will be included in the Computing programmes covering both safe school and home use.
All users will be informed that network and Internet use will be monitored.

How will the policy be discussed with staff?
The e-safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and pupils, the school will implement Acceptable Use Policies.

Staff that manage filtering systems or monitor ICT use will be supervised by the School Improvement Team and have clear procedures for reporting issues.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

How will parents' support be enlisted?

Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.

Equal Opportunities and Race Equality:

The governors and staff are committed to providing the full range of opportunities for all staff, regardless of gender, disability. ethnicity, social, cultural or religious background. All pupils have access to the curriculum, and the right to a learning environment which dispels ignorance, prejudice or stereotyping.