Oldfleet Primary School

E-Safety Policy

Author	
Date	April 2017
Review Date	April 2019

Why write an E-Safety policy?

A school's E-Safety Policy must cover the safe use of internet and electronic communications technologies such as mobile phones and internet connectivity.

This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school's E-safety policy will operate in conjunction with others including policies for Pupil Behaviour, Anti Bullying, Curriculum, Data Protection, and especially Safeguarding Children plus any Home-School Agreement.

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented E-Safety Policy;
- Secure filtered broadband from Kingston Communications and an internal firewall provided by Smoothwall Communications.
- A school network that complies with the National Education Network standards and specifications.

Writing and reviewing the E-safety policy

The E-Safety Policy relates to other policies including those for ICT, Anti- Bullying and Child Protection.

The school has appointed an E- Safety Lead who works closely with Child Protection Co-ordinator

Our e-Safety Policy has been written by the E-Safety lead and checked and approved by school staff and Governors.

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 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 includes filtering which is monitored on a daily basis

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be shown how to safely publish and present information to a wider audience.

Pupils will receive specific e-safety lessons as part of their learning.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

School ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with the ICT Co-ordinator, ICT Governor, E Safety Lead and School Business Manager.

Pupils may only use approved e-mail accounts on the school system.

Pupils must *immediately* tell a teacher if they receive offensive e-mail.

Pupil email accounts must only be used for internal emailing

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 forwarding of chain letters is not permitted.

School e-mail accounts should only be used in school for educational purposes. No other e-mail accounts should be available to access in the school.

Published content and the school web site

Staff or pupil personal contact information will not be published. The contact details given online should only be the school office.

The head teacher, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Statutory governor information will be published on the website in accordance with DfE regulations.

Publishing pupil's images and work

Written permission from parents or carers will be obtained before photographs of pupils are published in any form.

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified.

Wherever possible and if deemed more suitable and appropriate, we use group photographs rather than full-face photos of individual children.

Pupils' full names will not be used anywhere on the Oldfleet Primary school Web site or other on-line space, particularly in association with photographs.

Work can only be published with the permission of the pupil and parents/carers.

Pupil image file names will not refer to the pupil by their full name.

Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use.

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, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

The school will work with the internet support providers to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-Safety Lead who will arrange for the site to be immediately blocked.

The E-Safety Lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing use

Pupils must ask permission from the supervising teacher before making or answering a video conference call.

Video conferencing use will be appropriately supervised for the pupils' age.

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 should note 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.

Pupil mobile phones are only allowed on the school site with the permission of the head teacher. If allowed on the site, mobile phones are handed into reception at the beginning of the working day, stored securely and returned to pupils at the end of the working day.

All parents/carers and visitors will be made aware that mobile phones should be switched off whilst on the school premises.

Protecting personal data

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

Policy Decisions

Authorising Internet access

All staff must read and sign the electronic information and communications policy

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

Any person not directly employed by the school will be given a guest password for the internet which can be tracked.

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*. Neither the school nor Hull LA can accept liability for any material accessed, or any consequences of Internet access.

The school will annually 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.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by The Head Teacher

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 (see schools complaints policy)

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

We currently do not have any community use of the school internet systems

Introducing the E-safety policy to pupils and staff

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in E-Safety will be developed and offered to all staff and pupils on a termly basis

Staff and the e-Safety policy

All staff will be given a copy of the School E-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff will always monitor a child's use of search engines when accessing the web.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School E-Safety Policy in the school information pack /brochure and on the school Web site.

The school will publish on the website a list of E-safety resources for parents and carers

The school will ask all new parents to sign the home/school agreement when they register their child with the school.

Appendix 1: Internet use –

Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories The school website
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Google Bing
Exchanging information with other pupils.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information.	Microstft365
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on 'moderated sites' and by the school administrator.	The school website
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	The school website TWITTER Marvellous Me Digitull
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	None approved

Appendix 2: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Published on the school website