



Wick CE Primary School E-Safety Policy

Introduction

The Internet offers great experiences for adults and children. There are opportunities to improve your life, have some fun, enhance your education or pursue business interests. Nowadays, young people are often enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid.

Aims

Why Internet use is important

The Internet is an essential element in 21st century 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. 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 is 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. 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Guidelines and Expectations

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly with our service provider.

Virus protection is updated regularly.

Advice on security strategies will be monitored and discussed with our service provider.

E-mail

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.

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

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

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 will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully.

Pupils' full names will not be used anywhere on the Web site, 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.

Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

The school will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the LA, DCSF, SWGFL and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the ICT Coordinator.

ICT Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

When this becomes available within the school, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing 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.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Personal data will be 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 'Acceptable Use Agreement' before using any school ICT resource. (See Appendix C)

All parents will be asked to sign and return the 'Pupil Acceptable Use Agreement and E-Safety Rules' and internet consent form. (See Appendix B)

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

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

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor SGCC can accept liability for the material accessed, or any consequences of Internet access.

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

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff and noted on the incidents of misuse form. (See Appendix A)

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.

Communications Policy

Introducing the E-safety policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

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.

Enlisting parents' support

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

Review

This policy will be reviewed by the curriculum committee every year, or earlier if considered necessary.

Written by: Robert Cockle

Date: 2/4/21

Approved by: H+S and Curriculum Committee

Date: 20/4/21

Reviewed by: H+S and Curriculum Committee

Date: 20/4/21

Next review: April 2024

Signed..... Date

Chair of H+S and Curriculum Committee

Appendix B

Pupil Acceptable Use Agreement / E-Safety Rules

Dear Parent/Carer

We are currently reviewing the children's safety around school. ICT including the internet, email, laptops, digital cameras etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Could you please discuss these E-Safety rules with your child and sign the form and return it school as soon as possible.

- I will only use ICT in school for school purposes.
- I will use the internet in a safe and secure manner.
- I will only use my class email address. (if available)
- I will make sure that all ICT contacts with other children and adults are responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will follow the Hector procedures and tell my teacher immediately.
- I will not send to children or adults anything that could be considered unpleasant or nasty.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carers contacted if a member of school staff is concerned about my E-Safety.

Parent/Carer signature

We have discussed this and _____ (child's name) agrees to follow the E-Safety rules and to support the safe use of ICT at Wick CE Primary School.

Parent/Carer Signature _____ Date _____

Appendix C

Staff Acceptable Use Agreement / Code of conduct

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT co-ordinator, School E-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues material that could be considered offensive or illegal.
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date

Full Name
