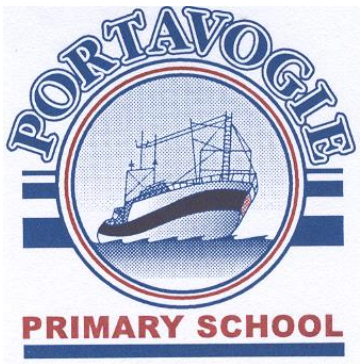
PORTAVOGIE PRIMARY SCHOOL



E-SAFETY POLICY

Contents:

Agreed with Chairperson of Board of Governors, Principal, School Council and E-Safety Committee

Rationale

To safeguard and promote the welfare of pupils; and
(Article 17 of the Education and Libraries (Northern Ireland) Order 2003).
determine the measures to be taken at a school to protect pupils from abuse)

(*Article 18 of the Education and Libraries (Northern Ireland) Order 2003).*
The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The school has a duty of care to enable pupils to use on-line systems safely. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. It covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.
This policy is largely based on DENI Circular 2007/1 *'Acceptable Use of the Internet and Digital Technologies in Schools' and DENI Circular 2011/22 'e-Safety Guidance' and* should also be read in conjunction with the School's Safeguarding policies.

Aims: What is e-Safety?

E-Safety (electronic safety) in the school context:
is concerned with safeguarding children in the digital world, with an emphasis on learning to understand and use technologies in a positive way;

is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;

is concerned with supporting pupils to develop safer online behaviours both in and out of school; and

is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

ICT is a compulsory cross-curricular element of the NI Curriculum and the school must ensure acquisition and development by pupils of these skills. The Internet and digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The school provides pupils with opportunities to use the excellent resources, along with developing the skills necessary to access, analyse and evaluate them.

Introduction

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in the Portavogie Primary School and is brought to the attention of all stakeholders.
We aim to develop mature systems of e-Safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies. As new technologies are developed, the school will respond quickly to any potential e-Safety threats posed by their use. The policy has been drawn up by the school's e-safety committee.

E-safety Committee:

Mrs Victoria Murray (Principal)
Mrs Kim Spence (Designated Child Protection Teacher)
Miss Joanne Johnston (ICT Co-ordinator)
School Council (Pupil Representatives)

The policy has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed bi-annually.

1.Internet Services

1.1 Connectivity and Filtering

The Internet is available using PCs, laptops and Ipads. Internet access is filtered for all users.

1.2 C2K

(C2k) is responsible for the provision of an ICT managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Internet use is monitored. Access to the Internet via the C2k Education Network is fully auditable and reports are available. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

Some of the safety services include:

- Providing all users with unique user names and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Filters access to web sites

2. Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. Staff and pupils are made aware that use of the school's ICT resources is a privilege which can be removed.
The school has a 'Guidelines for the Use of the Internet and Digital Technology' containing e-Safety Rules which makes explicit to all users what is safe and acceptable and what is not.
The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones) is subject to the same requirements as technology provided by the school.

2.1 Code of Safe Practice for Pupils

A parental/carer consent letter for pupils, is issued to parents/carers at the beginning of the new school year. This consent must be obtained before the pupil accesses the internet.
The following key measures have been adopted to ensure pupils do not access any inappropriate material:
The school's e Safety Code of Practice for Use of the Internet and other digital technologies is made explicit to all pupils;

E-Safety guidelines are displayed prominently throughout the school;

Pupils and their parents/carers are asked to sign the Code of Conduct sheets;

Pupils, using the Internet, will normally be working in highly-visible areas of the school;

All online activity is for appropriate educational purposes and supervised, where possible;

Pupils will, wherever possible, use sites pre-selected by the teacher and appropriate to age group;

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.
Use of mobile phones by pupils is not permitted on the school premises during school hours.

2.2 Pupil Sanctions

We believe it is important that the school has a culture under which users understand and accept the need for e-Safety regulations and adopt positive behaviours, rather than one in which attitudes are determined solely by sanctions. Incidents of technology misuse which arise will be dealt with in accordance with the school's Behaviour Policy.

Minor school related incidents may result in parents being informed and a temporary ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's Safeguarding Child Protection Policy.

Users will understand their responsibilities to report e-safety incidents. They will know and understand that there are clear systems for reporting abuse and understand that the processes must be followed rigorously. Incident reports will be logged by Mrs Hughes for future auditing, monitoring, analysis and for identifying serious issues or patterns of incidents. This will allow the school to review and update e-Safety policy and practices.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately. Users have an understanding of how to report issues online, including to CEOP.

2.3 Code of Safe Practice for Staff

The Code of Safe Practice has been agreed with staff.

Pupils accessing the Internet should on the whole be supervised by an adult at all times.

Staff will make pupils aware of the rules for the safe and effective use of the Internet.

Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to ICT Co-ordinator

In the interests of system security, staff passwords should only be shared with the network manager, ICT Co-ordinator

Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.

Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.

Photographs of pupils should, where possible, be taken with school equipment and images stored, accessible only to teaching staff or under supervision for pupil work.

School systems may not be used for unauthorised commercial transactions.

A Staff Safe Code of Conduct, which details sanctions, is signed by all staff.

3. Internet Safety Awareness

We believe that, alongside a written e-Safety Policy and Guidelines for the Use of the Internet and Digital Technology, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication, both inside school and outside school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

3.1 Internet Safety Awareness for Pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are signed by parents and pupils. Posters are on display.

Resources:

Child Exploitation and Online Protection (CEOP) resources: a useful teaching tool looking at Internet safety and incorporated into our PDMU and ICT programme.

Childnet International www.childnet.com has produced materials to support the teaching of e-Safety at Key Stage One and Two. They have materials for parents and staff too.

Other pupil resources available:

Superclubs, 360 e Safety Tool, *Signposts to Safety, KidSMART, Know IT All for Schools, ThinkUKnow*

3.2 Internet Safety Awareness for Staff/ Professional Development

Teachers are the first line of defence in e-Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. E-Safety training is therefore an essential element of our staff induction and part of an on-going Continuous Professional Development programme. Through our e-Safety policy, the school can ensure that all reasonable actions are taken and measures put in place to protect all users.

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. Staff uphold copyright regulations and intellectual property rights.

3.3 Internet Awareness for Governors

Mrs Murray keeps governors updated on e-Safety and any e-safety issues.

3.4 Internet Safety Awareness for Parents/ Carers and the Community

The 'Acceptable Use of the Internet' for pupils and Acceptable Use Agreement is sent home at the start of each school year for discussion with their child and parental signature. This e-Safety Policy is available on the school website. Internet safety leaflets for Parents/carers' attention are sent home when issued to school. Parents are informed of the school's complaints policy which is on the school website.

4. Health and Safety

We have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and the ICT suite, which has been designed in accordance with health and safety guidelines and where pupils are supervised at all times. Guidance is issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy. (see separate policy 'Health and Safety in ICT')

4.1 Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. The school, to the best of its knowledge, has considered all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use.

4.2 Use of Mobile Phones

Pupils do not bring mobile phones to school.

4.3 Digital and Video Images

Parental permission is gained when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached). Digital images are securely and disposed of in accordance with the Data Protection Act. Parental Consent forms for photos, videos, child on the website / newspaper is sent out at the beginning of the year. These must be signed and returned to school.

4.4 Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available on The Health Protection Agency website.

4.5 Personal Data

The school ensures all staff know and understand their obligations under the Personal Protection Act and comply with these to ensure the safe keeping of personal data, minimising the risk of loss or misuse of personal data.

4.6 Social Media

Care will be taken when making use of social media for teaching and learning. While social media technologies can offer much to schools and pupils, however each brings its own unique issues and concerns. Each social media technology that is to be utilised will be risk assessed in the context of each school situation. Teachers are the only users who have access to Social Media.

4.7 Cyber Bullying

Staff are made aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the schools overall Anti-Bullying policy and Pastoral Care Policy as well as the e-Safety Policy.
Cyber Bullying can take many different forms and guises including:
 Email – nasty or abusive emails which may include viruses or inappropriate content.

 Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.

 Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.

 Online Gaming – abuse or harassment of someone using online multi-player gaming sites.

 Mobile Phones – examples can include abusive texts, video or photo messages. Sexting occurs in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.

 Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

 Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils will be reminded that cyber-bullying can constitute a criminal offence.

While there is no specific legislation for cyber-bullying, the following covers different elements of cyber-bullying behaviour:
Protection from Harassment (NI) Order 1997 http://www.legislation.gov.uk/nisi/1997/1180
Malicious Communications (NI) Order 1988 http://www.legislation.gov.uk/nisi/1988/1849
The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

Pupils are encouraged to report incidents of cyber-bullying to their parents and the school. If appropriate, the PSNI may be informed to ensure the matter is properly addressed and behaviour ceases. The school will keep records of cyber-bullying incidents to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

School Website

The school website www.portavogieps.co.uk is used to celebrate pupils' work, promote the school and provide information. The website reflects the school's ethos. Information is accurate and well presented and personal security is not compromised. The principal and teachers edit the website.

The following rules apply:
The point of contact on the website is the school address, school e-mail and telephone number.

Staff or pupils' home information will not be published.

Website photographs that include pupils will be selected carefully. Parents who prefer their child's photographs do not appear on the school website is respected.

Pupils' full names will not be used in association with photographs.

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

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Monitoring and Self Evaluation

The school's wider self-evaluation processes (such as for an incoming School Development Plan) will address e-safety in the overall ICT and Safeguarding Child Protection Policy reviews. All key stakeholders are part of the self-evaluative review. Pupils offer a voice through school council meetings. Monitoring records of e-safety incidents are presented to the Governors. This policy will be reviewed and amended in light of evidence provided by monitoring, updated technologies or new DE Guidance.

This policy should be read alongside the following: Pastoral Care Policy, Positive Behaviour Policy, Safeguarding Child Protection Policy, Anti Bullying Policy, Health and Safety Policy and the ICT Policy.

Staff Safe Code of Conduct:

ICT (including data) and the related technologies such as e-mail, internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with the Principal and ICT Co-ordinator.

✓ I will only use the school's email or personal email (if approved by the Principal)/ Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.

✓ I will comply with the ICT system security and not disclose 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 not give out personal details e.g. mobile phone number and personal e-mail address, to pupils.

✓ I will ensure personal data is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors.

✓ I will not install any hardware or software on the C2K system without the permission of the Principal .

✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on the C2K system or on the iPads.

✓ Images of pupils and/or staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.

✓ I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Principal and ICT Co-ordinator. (managers).

✓ I will respect copyright and intellectual property rights.

✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

✓ I will support and promote the school's e-Safety and Data Security policies 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 practice and to support the safe and secure use of ICT throughout the school

Staff Member:……

Job Title:……

Think then Click!

(e-Safety Rules for Foundation and KS1)

These rules help us to stay safe on the Internet

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

Think then Click

(e-Safety Rules for Key Stage 2)

 We ask permission before using the Internet.

 We only use websites that an adult has chosen.

 We tell an adult if we see anything we are uncomfortable with.

 We immediately close any webpage we are not sure about.

 We only e-mail people an adult has approved.

 We send e-mails that are polite and friendly.

 We never give out personal information or passwords.

 We never arrange to meet anyone we don't know.

 We do not open e-mails sent by anyone we don't know.

 We do not use Internet chat rooms.

S **Secret:** Never give out your address, telephone number, username or password when on-line.

M **Meeting** someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher.

A **Accepting** e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.

R **Remember** no offensive language, text or pictures are to be displayed, sent, copied or received.

Be SMART Online

teacher or trusted adult if someone

Appendices

Appendix 1 – Guidelines for the Use of Internet and Digital Technologies (Parent and Pupils)

Appendix 2 – Staff Code of Conduct

Appendix 3 – Foundation and Key Stage 1 E-Safety Poster

Appendix 4 – Key Stage 2 E-Safety Poster

Appendix 5 –E-Safety Poster – Be SMART online