E-Safety Policy

Signed: _____

(Principal)

Signed: _____

(Chair of Board of Governors)

Date:_____

Introduction

The creative use of ICT, when used both in school and in the home, has the potential to transform and enrich children's learning experiences and to encourage them to become independent, self-motivated and flexible learners. (NI Curriculum)

At School

In Naíscoil & Gaelscoil Éadain Mhóir, pupils will be given the opportunity to develop their ICT skills by engaging in meaningful research and purposeful, curriculum-based activities to:

Explore **E**xpress **E**xchange **E**valuate & **E**xhibit

their work and learning using ICT.

We have invested heavily in the purchase of additional ICT resources in recent years and our pupils have access to a range of ICT based electronic devices, including:

PCs, Laptops, Interactive Whiteboards, I-pads, Bee-Bots, Microphones etc.

ICT based activities include:

Use of educational apps

Use of interactive games

Research as part of topic based work

Sound / Video recording

Photography

Videography

Podcasting (Seomra Nuachta / Newsdesk)

Use of music / video downloads

Training

Our staff have received training in the use of the Interactive Whiteboard, I-pads, and e-safety.

Parents and children in Ranganna 5-7 have received sessions of e-safety training, provided by external agencies. (Bogside & Brandwell Health Forum)

At Home

We recognise that many of our pupils have access to a range of ICT based devices and resources, which can be used both in and out of the context of education.

For example:

Mobile / Smart phones, Gaming machines (Play Stations, Wii, x-box etc), I-pads, I-Pods, Tablets etc.

Many children are also beginning to use internet based technologies for the purposes of:

Social Networking, e mail, instant messaging, chat rooms, blogs, video / music downloading etc

Aim of Policy on E-safety, Images and Acceptable Use of Internet

Whilst ICT resources / Web-based programmes can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

The aims of this policy are:

- to raise awareness among teachers, parents and pupils of the potential risks involved with internet / ICT useage, both in school and at home
- to ensure that school staff, parents and pupils are aware and agree with the guidelines on the 'Use and Storage of Images' and on 'Acceptable Use of the Internet'
- to outline the measures and educative work taking place in the school to protect our pupils
- to teach our pupils how to make positive use of ICT and internet related technologies to enhance their learning,
- to encourage our pupils to learn how to remain both safe and legal and to display appropriate behaviour and etiquette when online in the class-room and beyond

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key Concerns are:

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons.

Children should be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details or
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet, there are unsuitable materials in many varieties. Anyone can post material on the Internet.
Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.
Materials may express extreme views. e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

Materials may contain misleading and inaccurate information. e.g. some use the web to promote activities which are harmful such as suicide, anorexia or bulimia.

Children should be taught:-

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a parent / teacher / adult immediately.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership and of the Safeguarding ethos within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal / ICT Co-ordinator update Senior Management and Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the e-safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Parental Permission, Positive Behaviour, Child Protection, and Anti-bullying.

The e-safety policy and its implementation will be disseminated among parents for consultation via our website / discussion with members of Cairde na Gaelscoile and will be reviewed bi-annually or in light of updated guidance form the relevant authorities.

E-safety Skills' Development for Staff

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on e-safety
- All staff are encouraged to incorporate e-safety activities and awareness within their lessons.

E-safety Information for Parents/Carers

At School

- Parents are asked to sign a permission slip on an annual basis regarding use of ICT / Internet resources and use of photographic images of their children.
- Parents / carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child. Please also discuss the implications of this agreement with your child.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used on the school website.
- The school website will contain useful information and links to sites like CEOP's **thinkuknow**, **Childline,** and the **CBBC Web Stay Safe** page.
- The school will communicate relevant e-safety information through newsletters and the school website / text system.
- Parents have also been invited to attend e-safety training

At Home

Parents are encouraged to:

- make responsible decisions regarding the purchase of mobile devices / ICT based equipment for the home, taking into consideration the age and stage of development of their child.
- install parental controls / internet filtering on their home broadband service.
- remember that it is important to promote e-safety in the home and to monitor Internet use.
- keep the computer in a communal area of the home and let your child see that you are keeping an eye on their use of the internet.
- be aware that children have access to the internet via gaming stations and portable technologies such as smart phones and can be invited to play against others.
- monitor on-line time and be aware of excessive hours spent on the Internet or on gaming devices, as this can have a detrimental effect on children's attention and focus.
- take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.

- advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.

- discuss the fact that there are websites / social networking activities which are unsuitable and to be aware of the recommended age limits for apps súch as facebook, snapchat and instagram.

- discuss how children should respond to unsuitable materials or requests.

- remind children never to give out personal information online.

- remind children that people on line may not be who they say they are.

- be vigilant. Ensure that children do not arrange to meet someone they meet on line.

- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

E-safety Information for Teachers / School Staff

C2k Accounts

- All teachers, support staff and pupils have their own c2k login (username and password) and should only use the computer when logged in under their own password. Staff members should not share their login details.

- All substitute teachers will be given login details and will be asked to read the e -safety policy and sign the 'Acceptable Use of the Internet' agreement as part of their induction.

- Staff should ensure that children do not know the login details of staff and do not use the computer when a staff member is logged in, as staff may have a higher level of internet access than children. If by chance, a child gains access to a staff member's password, the c2k manager should be informed and the password changed immediately.

Internet use at school:

- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult.

- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

- The school will plan and provide opportunities within a range of curriculum areas to teach e-safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- Pupils will be taught what type of 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.

- 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.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.
- Video / Music material which is downloaded from the Internet must be viewed in full by the teacher prior to being shown to the pupils, to ensure that the content is suitable and that 'pop-up' adverts etc so not arise which may be inappropriate.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- 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.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

Pupils:

- The school C2k system will block access to all social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still be allowed to use them, or may use them without the knowledge of their parents. They will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.

Staff:

- School staff are advised not to use social media to communicate with parents of children in the school and are advised not to 'be-friend' parents on social media. However, we recognise that staff may have personal relationships / be related to parents of the school and may use social media to communicate with them on a personal level.
- School staff must not under any circumstance add pupils of the school as 'friends', if the pupils use social media sites.
- Past-pupils of the school should not be added as 'friends' on social media by staff members if they are under the age of 18 years.
- Staff are advised not to post comments regarding the school, pupils or their place of work on social media.

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to bring personal mobile devices / phones to school under any circumstance.
- Staff should not use personal mobile phones during designated teaching sessions.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Digital Images

- Digital images of pupils will only be taken using school based equipment and will not be taken using personal equipment owned by a staff member eg. personal mobile phone / i-pad.

- Digital images will only be stored on school-based devices and not stored by staff on personal memory pens or portable hard-drives which could potentially be removed from the school.

- If photographs are to be printed, this will be done in school or in a local chemist, by a staff member. The i-pad / memory card / storage device will not be left unattended in the shop during printing.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This consent form is considered valid for the entire school year, unless there is a change in the child's circumstances where consent could be an issue. It is the responsibility of parents to notify us of such changes.
- Parents / carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and pupils' full names will not be published under photos.
- Pupil's work can only be published by outside agencies, such as local newspapers, with the permission of parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-safety rules. These e-safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-safety rules and within the constraints detailed in the school's e-safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling e-safety Complaints:

- Complaints of Internet misuse will be dealt with by the Principal and ICT co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT co-ordinator and recorded in the e-safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal and the Chair of the BOG will be informed.
- 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.

Communicating the Policy:

Introducing the e-safety Policy to pupils

- e-safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons / circle times / anti-bullying week.
- 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.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop / iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Principal and ICT Co-ordinator.

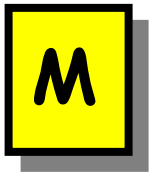
This policy will be ratified by the Board of Governors and they will review its effectiveness bi-annually.

Internet Safety Rules for Children

Please place this e-safety poster in a visible place in your home, eg. beside the computer or charging station.

Follow These SMART TIPS

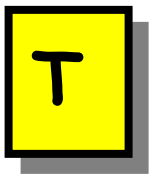
Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees