An e-Safety Policy

St Patrick's PS Annaghmore

In all schools there is a need to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."

Dr Tanya Byron Safer children in a digital world: The report of the Byron Review

It is essential that teachers, parents, Boards of Governors and pupils are all aware of e- Safety and are involved in devising and discussing appropriate strategies for the safety of all users.

Caroline McFall ICT Coordinator St. Patrick's PS Annaghmore

What is the Internet?

The Internet is a huge network of computers making a worldwide community. It is a way of connecting computers together so that people using them can:

- talk to each other,
- send and receive messages,
- obtain information and resources,
- publish information,
- buy and sell things and
- Have fun.

ICT

The term, Information and Communications Technology (ICT) covers a range of resources from traditional computer-based technologies to the fast-evolving digital communication technologies.

Some of the Internet-based and electronic communications technologies which children are using, both inside and outside of the classroom, are:

- Websites
- Learning Platforms / Virtual Learning Environments
- Email and Instant Messaging
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting - Skype/Facetime
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality

- IPads and other tablet devices with internet access

While these ICT resources 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 their use.

The World Wide Web (WWW)

The World Wide Web (WWW) or Web provides easy access to the vast quantity of information and resources available on the Internet and is the facility which people use to "surf" for information. It is made up of millions of screens or pages of information.

The collection of pages created by one individual or organisation is known as a website. Each page can include text sound, images, animation and video and has its own unique address.

E-Mail

E-mail allows users to send and receive written messages.

Chat Rooms

Chat rooms allow a number of people to "meet" on the Internet. It is similar to having a telephone conversation with a number of people at one time except that the participants type instead of talk.

Social Media

Social Media sites are ever changing and ever increasing. At present children have access to sites such as Facebook, Twitter, Instagram, Snapchat, and Flickr to name but a few

The Internet is often described as being like a vast city. It is an exciting place with a great variety of places to visit. There are shops, entertainment areas, educational areas and people

to meet. But it also contains dangers. There are areas that we do not want to go to and that we certainly would not want children to visit.

E-Safety

E-Safety encompasses internet technologies and electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

DENI Safeguarding and Child Protection in Schools: A guide for Schools (May 2017)

"Online safety is about using digital devices in a smart but safe way. It means educating children and young people to act responsibly and keep themselves safe in the digital world." *C2K Support Materials on Fronter (May 2017)*

- E-Safety concerns safeguarding children and young people in the digital world.
- E-Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more on education about the risks as well as the benefits so pupils can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

In St Patrick's Annaghmore, we understand our responsibility to educate pupils in e-Safety. We aim to teach children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

How Valuable is the Internet in Education?

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.

- It gives children opportunities to locate, retrieve and exchange information.
- It encourages the development of ICT skills that are vital to life-long learning.
- It takes learning beyond the classroom.
- It allows access to stores of information that might otherwise be unavailable in school.
- It provides up-to-date information.
- It is a fast and efficient way of communicating and retrieving information.
- It encourages independent learning.
- Children enjoy using it.
- It is part of their life experience.

The Internet is increasingly part of our work, home, social and leisure activities. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world.

Risks and Responses

The Internet is an 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
In our school children will 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
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information (e.g. send inappropriate photographs) 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 anorexia or bulimia.

In our school children will 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 teacher/adult immediately.

Cyber Bullying

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites. If it takes place within school, cyberbullying will be dealt with in line with the school's overall anti-bullying policy, discipline policy and pastoral services.

In our school children will be taught:

- If they feel they are being bullied by e-mail, through social networking sites, text or online they should always tell someone they trust.
- Not to reply to bullying, threatening text messages or e-mails as this could make things worse.
- Not to send or forward abusive texts or e-mails or images to anyone.
- Keep abusive messages as evidence.

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school

We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership 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. Miss McGuinness/Mrs McFall have responsibility for leading and monitoring the implementation of e-Safety throughout the school.

Circulars relating to online safety e.g. DENI Circular 2016/17 'Online Safety', Circular 2016/26 Effective Educational Uses of Mobile Digital Devices, are saved for reference in the staff folder and all staff are made aware of where they can be found.

The Principal/ICT Coordinator 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, governors, 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, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The e-Safety Policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
- 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 the school's e-Safety Policy and Acceptable Use Agreement as part of their induction.
- All teachers are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

Parents/carers have an important role to play in promoting e-Safety. We encourage all parents/carers to become involved in e-Safety discussions and activities with their child.

- The school website contains links to sites such as CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page which parents can use with their children
- The school communicates relevant e-Safety information through parents' evenings/newsletters and the school website.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement with their child.

- Parents/carers are required to give written consent to images of their child being taken/used on the school website.

Parents are reminded regularly that it is important to promote e-Safety in the home and to monitor Internet use. The following guidelines are provided:

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- 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 and the "Click Clever, Click Safe" code
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- 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.

Teaching and Learning

Internet use:

- Teachers will plan for and provide opportunities across the curriculum for children to develop their e-Safety skills.
- Educating children 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.
- Children are made aware of the impact of online bullying and know how to seek help if these issues affect them. Children are also 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.
- The school Internet access is filtered through the C2k managed service using a Websense filtering solution.
- Websense assesses all websites based on their content and adds them to a category. (Green – available, Red – unavailable) All users are given access to a core group of green sites. The school has the facility to customise security options where need arises. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

- 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.
- Children are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Children are 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.
- 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. They will be taught to be "Click Clever, Click Safe":

  Zip it (never give personal data over the internet)
  Block it (block people you don't know)
  Flag it (if you see something you don't like flag it up with someone you trust).

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.
- Forwarding chain letters is forbidden.

- Sending or displaying insulting or offensive messages/pictures is forbidden.
- Using obscene language is forbidden

Social Networking:

- An increasing number of children are indicating that they have access to, or regularly use social media platforms such as Snapchat/ Facebook. Parents/Guardians are reminded that these platforms are age restricted and it is the view of our school that thy should never be used by primary school children
- However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Parents must be aware if they purchase devices for their children that they are responsible for their online safety using these devices

- 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.
- School staff will not add children as 'friends' if they use these sites.

Portable Technologies:

- The use of portable devices 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 use personal mobile phones during class.
- Be aware of the safety issues regarding mobile phones. Increasingly these have Internet access.

- Encourage children to talk about how they use mobile phones. Remind children not to give mobile numbers to strangers and people they do not know very well. Talk about responsible use of text messaging/images etc.
- Staff should not use personal mobile phones during designated teaching sessions.

Enhancing and Transforming Learning and Teaching (Circular 2016/26)

- The following four categories are ways in which mobile digital devices may be integrated significantly to enhance and transform aspects of learning to real advantage:
- Capturing and collecting information and experiences across a variety of settings, through photos, audio and video recordings, numerical and text entry.
- Communicating and collaborating with others via Fronter, and email.
- Consuming and critiquing media including music, photos, videos, games and text documents.
- Constructing and creating personal forms of representation and expression through edited photos and videos, sketches, podcasts, blogs etc.

- In St. Patrick's PS we have some specific learning activities which mobile learning can valuably enable. Pupils can:
- **Review and reflect:** pupils capture audio, imagery and video during lessons, use these in plenary sessions e.g.in structured play to reflect on an activity, consider the key elements learned, how these fit into wider subject or topic pictures and how ideas might be used or taken further outside the classroom. **Think forward:** pupils access future topic material via the Internet and capture relevant thoughts or ideas (research) to contribute to discussions or presentations in class or through on-line discussions.
- **Listen to my explanations:** pupils record audio when they are completing class work and these verbal explanations are listened to by teachers and peers.
- **Snap and show:** pupils capture imagery, which can be copied to our network and accessed through a computer or interactive whiteboard screen, for wider pupil discussion.
- **This is what I've done and how I've done it:** pupils create presentations using mobile technologies for particular activities, which are recorded and made accessible for teachers and parents to see.
- **Tell me how I could improve this:** pupils can share their work in multimedia formats with peers, teachers or trusted adults to seek comments, evaluative feedback, assessments of their work and ideas to improve their work.

iPads

- iPads are used for digital storytelling, internet research, and to support learning and teaching across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet Wise and apply the Internet safety rules.

  Prohibited use of iPads, Smart Phones, iPods etc.
- All material on the iPad must adhere to St.Patrick's Online Safety Policy. Users are not permitted to send, access, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- St. Patrick's internet/ email accounts may not be used for financial or commercial gain or illegal activity.

- Violating Copyrights - users are not allowed to have music and install apps on their iPad.
- Cameras - users must use good judgement when using the camera on iPads. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any misuse of mobile digital devices e.g. camera in toilets or changing room, regardless of intent, will be treated as a serious violation and will be dealt with in line with our Safeguarding and Child Protection Policy.

- Any misuse of mobile digital devices e.g. smart phones on online group chat forums will be dealt with in line with our Positive Behaviour Policy. Parents will be informed. .
- Images of people may only be used with the permission of those in the photograph.
- Take videos of pupils/staff without permission or direction from the teacher.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Management Team.
- Use of the camera and microphone, by pupils, is strictly prohibited unless permission is granted by a teacher.
- No user may gain access to another user's accounts, files or data.
- No user may attempt to destroy hardware, software or data.

- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- All users should be aware of and abide by the guidelines set out in St. Patrick's P.S Online Policy.

The Designated Teacher reserve the right to confiscate and search an iPad to ensure compliance with this Online Safety Policy

Managing Video-conferencing:

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

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website/local press/internally for display/externally for displays associated with the school. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and 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/guardians 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. They are encouraged to keep details of usernames and passwords private.
- 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 a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the teacher or ICT Co-ordinator and recorded in the e-Safety incident logbook.
- As part of the Acceptable Use Agreement children will know that if they deliberately break the rules they could be stopped from using the Internet/E-mail and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Complaints regarding cyberbullying will be dealt with in line with the school Anti-Bullying Policy.
- Pupils and parents will be informed of the complaints' procedure.
- Any complaint about staff misuse must be referred to the Principal and governors.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- e-Safety rules will be displayed in the ICT suite 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 involved in discussions regarding e-Safety and will have a copy of the e-Safety Policy.

- Staff will be aware that Internet use can be monitored and traced to the individual. 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.
- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone where contact with pupils or parents is required

Staff should follow the guidelines below:

- Never communicate with pupils outside of school via social networking sites and chat rooms.
- Never respond to informal, social texts from pupils
- Never use personal technology to take images or videos of children

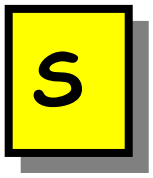
Monitoring and review:

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

This policy is the governors' responsibility and they will review its effectiveness annually. They will do this through liaison with the ICT Coordinator and the Designated Child Protection Coordinator.

Points for Children to Consider

Follow These SMART TIPS

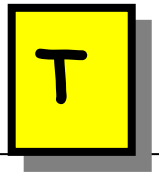


Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

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 Proctection Committee.

School Website

On our School Website:

- Children are only referred to by their first names.
- Any images of children will not be labelled with their name.
- Children and teachers will not reveal their personal details, home addresses or telephone numbers on the website.
- Children do not have individual e-mail addresses.
- Website links selected by teachers may be put on the website for pupils to access outside of school – sites will be previewed and checked regularly.

Parents'/Carers' permission will be sought to publish pupils work and/or photographs. These will only be published subject to the strict safeguards above.

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images.

Children are regularly reminded that should they encounter inappropriate material on line they must immediately

- Leave that website
- Inform an adult

Should a child or teacher encounter unsuitable material through the managed service, this will be reported to C2k via the C2k helpdesk number.

This policy has been reviewed in line with:
 DENI Circular 2016/27 "*Online Safety*"

Guidance Material on Internet Safety

http://schoolsl.becta.org.uk

www.ceop.gov.uk

www.thinkuknow.co.uk

Examples of safety rules for children are also available from:

http://www.kented.org.uk/ngfl/policy