SAINT EITHNE'S PRIMARY SCHOOL

E-Safety Policy
And
Acceptable Use Agreement

Date of Review: October 2022
Chair of Governors: _____

ICT

Information and Communications Technology (ICT) covers a range of resources from computer-based technologies to the ever 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 all users need to be aware of the range of risks associated with their use.

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.

- 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 about the education of 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 Saint Eithne's Primary School 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 safe when using the internet and related technologies, in and out the of the classroom.

Risks and Responses

The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. The Internet is, however, an open communications' channel, available to all. 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 fully destroyed although it is important to realise that if we act fast and remove the original posting as soon as possible, we can minimise damage.

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. Mrs Harrigan has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal/ICT Co-ordinator update 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 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 co-ordinator at staff meetings or planned CPD sessions .

- 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, Child.net and NSPCC which parents can use with their children
- The school communicates relevant e-Safety information through the school website and the school Facebook page.
- Parents/carers/guardians are asked to read through and sign the Acceptable Use Agreement with their child.
- Parents/carers/guardians are required to give written consent to images of their child being taken/used on the display boards in school, local newspapers, school website/facebook page

Parents/carers/guardians 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 on their mobile phone.

- 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.

- Discuss the fact that there are websites 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.

- Be aware that the minimum age for social media apps eg Facebook, Snapchat and Instagram is 13, this is in compliance with the US Children's Online Privacy Protection Act.

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/guardians, teacher/trusted member of staff, or an organisation such as Childline/NSPCC/CEOP.

- The school Internet access is filtered through the C2k managed service using a Websense filtering solution.

- 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 "SMART"

E-mail:

Only the Primary 6 and 7 children will have access to e-mail in school for 'exchange' purposes.

- 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:

- Through the C2k system our school currently blocks access to social networking sites.
- Pupils and parents /carers/guardians 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 use them; 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.
- 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.
- Staff should not use personal mobile phones during designated teaching sessions.

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. They will not be allowed to use iPads to:

- Take photos of pupils/staff without permission or direction from the teacher.
- Take videos of pupils/staff without permission or direction from the teacher.

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/guardians/carers will be obtained before photographs of pupils are published on the school Website/Facebook page. 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.

- 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/carers/guardians.

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.

- 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.

- Access to the Internet will be supervised.

- All parents/guardians/carers 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.
- 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/carers/guardians 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 all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers in the first term of every year and at relevant points throughout e.g. during PDMU lessons/circle times.

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/carers/guardians 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 Co-ordinator and the Designated Child Protection/Safeguarding Co-ordinator.

Safety Rules for Children

Follow These SMART TIPS

SMART Tips from: – https://www.childnet.com

An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents/guardians/carers are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.

- I will keep my username and password private.

- I will not access other people's files without their permission.

- I will not change or delete other people's work/files.

- I will ask permission before entering any website, unless my teacher has already approved that site.

- I will use the Internet for research and school purposes only.

- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.

- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.

- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.

- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.

- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

- I will not bring in memory sticks or mobile devices from home to use in school unless I have been given permission by my class teacher.

- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.

I

- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.

- I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/carers will be informed.

Saint Eithne's Primary School

Acceptable Use Agreement
For Pupils

Please discuss the Acceptable Use rules with your child and then complete and return this form to your child's class teacher

Pupil's Name		Class Teacher	
As a school user of the Internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
Pupil Name (print)			
Pupil Signature		Date	

Parent's/carers/ guardians Name			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.			
Parent's/carers/guardians Name (print)			
Parent's /carers/guardian signature		Date	

SAINT EITHNE'S PRIMARY SCHOOL

Acceptable Use Agreement
For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's e-Safety Policy has been drawn up to protect all parties – the children, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

➢ Internet use should be appropriate to staff professional activity or the pupils' education

➢ Access should only be made via the authorised C2K account and password, which should not be made available to any other person

➢ The C2k email account should be used for professional purposes.

➢ Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received

➢ Posting anonymous messages and forwarding chain letters is forbidden

➢ As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media

➢ Use of the network to access or send inappropriate materials such as pornographic, racist or offensive material is forbidden

➢ Use for personal financial gain, gambling, political purposes or advertising is forbidden

➢ Copyright of materials must be respected

➢ Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden

Name		
Date		**Signed**