St. John's Primary School
Gilford

E-Safety Policy
And
Acceptable Use Agreement

Policy Adopted: Autumn 2019
Next Review Date: Autumn 2020

Signed:_____
(Chair of Governors)

Date:_____

Introduction

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

Whilst 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.

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 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. John's 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.

The Internet

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

Children should be taught that:

- People are not always who they say they are.
- "Stranger Danger" applies to the people they encounter through the Internet.
- They should never give out personal details
- They should never meet alone anyone contacted via the Internet, and
- 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 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 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.

Children should 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. 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. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

The Principal/ICT Co-ordinator update staff 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.

The E-Safety Policy and its implementation will be reviewed annually or more frequently in light of changing circumstances.

E-Safety Skills Development for Staff

- All staff receive regular information and training on E-Safety issues through the co-ordinator 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/Guardians are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/Guardians 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 contains useful information and links to sites like CEOP's thinkuknow, Kid Smart, etc.
- The school will communicate relevant E-Safety information through newsletters and/or school website.

Parents/Guardians should remember 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.
- Pupils 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.
- 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.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils 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.
- Pupils 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.

Email:

- 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.

Social Networking:

- Through the C2k system our school currently blocks access to 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 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.
- Our school has a Twitter account @stjohnsgilford. This is used as a method of raising the School's profile and as a means of communication to parents.
- Pupils are not encouraged to set up their own Twitter accounts as a way of gaining access to the School's Twitter account.

Mobile 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 devices/phones in school. However, if a pupil does bring in a mobile phone this must be handed into the school office for safekeeping.
- Staff should not use personal mobile phones during designated teaching sessions.
- Staff will use school iPads/cameras for photographs. Personal staff devices may be used to take photographs for the purposes of the school website and Twitter account. Photographs will be deleted after uploading.
- A school mobile telephone will be used on school trips.

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. Pupils 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:

- Video-conferencing will be via the C2k network to ensure quality of service and security.
- Video-conferencing 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/School App or Twitter account. This consent form will be sought at the start of each academic year.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

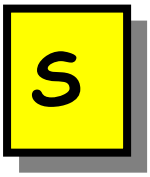
Monitoring and review:

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

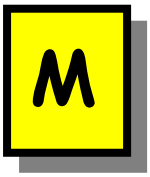
This policy is the governors' responsibility and they will review its effectiveness annually. They will do this through liaison with the ICT Co-ordinator and the Designated Child Protection Co-ordinator.

Safety Rules for Children

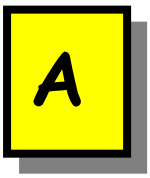
Follow These SMART TIPS



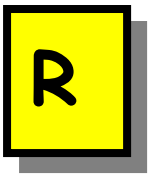
Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



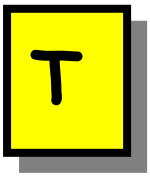
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



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.

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 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 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.

ST. JOHN'S P.S GILFORD

42A Castle Hill, Gilford, Craigavon BT63 6HH

Phone: 028 38831555 Email:info@stjohns.gilford.ni.sch.uk

Principal: Mrs S Lyness BSSc PGCE PQH(NI)

www.stjohnspsgilford.com Twitter:@stjohnsgilford

Acceptable Use Agreement

Dear Parent/Guardian,

We are currently updating our E-Safety Policy. Please find attached a leaflet containing some extracts from this policy. Before being allowed to use the Internet, all pupils must obtain permission and both they and you must sign and return the consent form as evidence of your approval and their acceptance of the school rules on this matter. **If you do not return your form your child will not be permitted to use the Internet in school.**
I would be grateful if you would read the attached leaflet and then complete the consent form.

Yours faithfully,

Sorcha Lyness

I have read and understood the school rules for responsible 'Internet Use' and give permission for my child _____ to access the Internet. I understand that the school will take all reasonable precautions to ensure children cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages from the use of the Internet facilities.

Signed: _____ (Parent/Guardian) Date:_____

Signed: _____ (Pupil P4/P7) Date:_____

Permission for Use of Images

I give permission for my child's/children's' image to be used for the following:

- School Website
- School Twitter Account
- School App
- Parish Website
- Local Newspaper
- Other outside agencies

Signed: _____ (Parent/Guardian) Date: _____

St. John's Primary School, Gilford

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-mails sent and for contacts made that may result in e-mails being received
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mails can be forwarded or inadvertently 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**

St. John's Primary School Gilford

E-Safety Incident Log Book

Date	Name of person involved	Incident reported	Action taken and signature