St. Ronan's Primary and Nursery School

E-Safety Policy

&

Acceptable Use Policy

(Including Acceptable Agreement)

Signed _____ (Chair, BoG)

Date _____

Policy Updated: 25 February 2019 **Review Date:** February 2022

Rationale

Boards of Governors have a duty to:

- Safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries N. I. Order 2003).
- Determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries N.I. Order 2003).

In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.

ICT

Information and Communications Technology (ICT) covers a wide range of resources including traditional computer – based learning and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

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

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 the use of Internet technologies.

In St. Ronan's Primary and Nursery School, we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them 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.

E-Safety: Electronic 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.

- Concerned with safeguarding children and young people in the digital world; emphasises learning to understand and use technologies in a positive way;
- Less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- Concerned with supporting pupils to develop safer online behaviours both in and out of school;
- Concerned with helping pupils recognise unsafe situations and how to respond appropriately.

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern.

This e-Safety policy reflects this by keeping abreast of the changes taking place. The school has a duty of care to enable pupils to use on-line systems safely. This e-Safety policy contains aspects in relation to use of the internet, use of mobile phones and use of digital/photographic images of children. It is largely based on DENI Circular 2007/1 *"Acceptable Use of the Internet and Digital Technologies in Schools"*, DENI Circular 2011/22 *"Internet Safety"* and DENI Circular 2013/25 *"e-Safety Guidance".*

It should also be read in conjunction with the School's Safeguarding Policies.

ICT is a compulsory element of the NI Curriculum and schools must ensure acquisition and development by pupils of these skills. 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. Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.
The DENI circular 2007/01 states that:
"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in St. Ronan's Primary and Nursery School. We aim to develop systems of safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies. The policy has been drawn up by the staff of the school under the leadership of Mr McGrath (Principal) and ICT Co-ordinator. It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed annually.

Internet Services

Connectivity and Filtering
The school has an internet system (C2K) which filters illegal content for all users.

C2k
Classroom 2000 (C2k) is the project responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Some of these safety services include:

- Providing all users with a unique user names and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses Filters access to web sites
- Providing appropriate curriculum software.

Should the school decide to access online services through service provider's other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

Code of Safe Practice
When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. We have a Code of Safe Practice (Appendix 1) for pupils and staff (Appendix 2) containing e-Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile

phones, camera phones, PDAs) is subject to the same requirements as technology provided by the school.

The ICT Co-ordinator and the Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

A parental/carer consent letter (Appendix 3) accompanied by the code of practice for pupils is sent out annually to parents/carers at the beginning of the school year and for any child in Years 4 – 7 who joins the school throughout the school year. This consent must be obtained before the pupil accesses the internet.

In addition, the following key measures have been adopted by St. Ronan's Primary and Nursery School to ensure our pupils do not access any inappropriate material:
The school's e-Safety code of practice for Use of the Internet and other digital technologies are made explicit to all pupils and e-Safety guidelines are displayed prominently throughout the school;

- e-safety guidelines are displayed prominently throughout the school;
- Our Code of Practice is reviewed each school year and signed by pupils/parents;
- Pupils using the Internet will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils in Years 4 -7 are educated in the safe and effective use of the Internet, through a number of selected websites;
- Pupils will not access social networking sites in school.

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

Pupil Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/ Positive Behaviour Policy. Minor incidents will be dealt with by Mr McGrath and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's Child Protection Policy.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff: (An example of an ICT Safe Code of Practice Agreement which staff can be asked to sign when taking up post is attached for information)

- Pupils accessing the Internet should be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinator.
- In the interests of system security staff passwords should only be shared with the network manager.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should, where possible, be taken with a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work.
- School systems may not be used for unauthorised commercial transactions.

Internet Safety Awareness

In St. Ronan's Primary and Nursery School we believe that, alongside having a written e-Safety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication both inside and outside the school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils. E-safety awareness will be fully embedded in all aspects of the curriculum.

Internet Safety Awareness for pupils

- Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms.
- 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/Internet Safety Day.
- Pupils will be informed that network and Internet use will be monitored.

- The school will provide e safety workshops for pupils and parents periodically.
- Key Stage 2 pupils are made aware and discuss Internet Safety through structured lessons using a range of on line resources e.g. ThinkUKnow, Child Exploitation and On-line Protection (CEOP), KidSMART.

Internet Safety Awareness for staff

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Departments policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.

The Child Exploitation and Online Protection Centre **(CEOP)** run regular one-day courses for teachers in Northern Ireland. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the Thinkuknow website.

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 Acceptable Use Agreement as part of their induction.
- All staff incorporate e-Safety activities and awareness within their lessons.

Internet Safety Awareness for Parents

The Internet Safety Policy and Code of Safe Practice for pupils is sent home at the start of each school year for parental signature. Additional advice for parents with internet access at home also accompanies this letter or Internet safety leaflets for parents and carers also are sent home annually. The school organises a biannual talk on Internet Safety, usually delivered by PSNI for pupils, parents and the community.

Health and Safety

In St. Ronan's Primary and Nursery School we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT

resources in classrooms which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Active Panels are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboard and Active Panels. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are also mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be protected. The school to the best of its knowledge has considered all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use. In doing so, pupils are informed of what to do if they come across inappropriate material on line.

Use of Mobile Phones

Most modern mobile phones have internet connectivity.

Digital and Video Images

- The school may publish on the school website or in the local newspaper, photographs that will celebrate an individual or group of children's achievements/success.
- The school principal, Mr McGrath, may also give permission for other bodies to use school photographs/children's photographs to celebrate or publicise their and the school's work.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website/FACEBOOK/Twitter/Newspapers/Other Publications. 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.

Wireless Networks

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

Cloud Storage

Data and information is stored on the Cloud, meaning it can be accessed from any location removing the need to carry data and files on memory pens and portable devices**.**

Web Site

The school web site www.stronansps.com promotes and provides up to date information about the school as well as is used to celebrate pupils' achievements. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well-presented and that personal security is not compromised. As the school's Web site can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply.

- The point of contact on the Web site should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site (see Digital Images policy section).
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Cyber Bullying

Staff at St. Ronan's Primary and Nursery School are aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is addressed within our school's Anti-Bullying Policy, Pastoral Care Policy as well as the e-Safety Policy.

Cyber Bullying can take many different forms and guises including:

- Email – Nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms- Potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – Typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – Abuse or harassment of someone using online multi-player

gaming sites.

- Mobile Phones – Examples can include abusive texts, video or photo messages.
- Abusing Personal Information – May include the posting of photos, personal information, fake comments and blogs or pretending to being someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyberbullying, the following legislation covers different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
- Malicious Communications (NI) Order 1988
- The Communications Act 2003

At St. Ronan's Primary and Nursery School, pupils are encouraged to report incidents of cyber-bullying to their parents and the school. If appropriate the PSNI may be informed to ensure that the matter is properly addressed and the behaviour ceases. The school will keep records of cyber- bullying.

Social Media and Networking

This is a generic term for community networks, chatrooms, instant messenger systems, online journals, social networks and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.

The majority of activity in these on-line social sites usually causes no concern. C2k filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment.

- The school C2k system will block 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 online 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.
- Pupils will not bring portable devices to school unless they have been instructed by their teacher.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile devices/ phones during class.
- Staff should not use personal mobile phones during designated teaching sessions.

Monitoring, Evaluating and Reviewing

- The policy will be reviewed and amended in light of updated technologies or new DE Guidance.
- 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.

Password Security:

- Staff members 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 ICT Coordinator and his team.
- 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.
- 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.

ICT Code of Safe Practice for Staff

E-Safety Rules

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

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, C2k, secure e-mail system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of ICT Co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of practice and to support the safe and secure use of ICT
throughout St. Ronan's Primary and Nursery School

Signature …….. Date ……

Points for Children to Consider

Follow These SMART TIPS

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

M **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.

A **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.

R **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!

T **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 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 (KS2 Only) 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 (KS2 Only) 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 any other memory 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/email and my parents/cares will be informed.

Parents are asked to read the acceptable use of the Internet agreement through with their children and complete the following forms as necessary.

Children's acceptable use of the Internet agreement:

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:	

Parents acceptable use of the Internet agreement.

Pupil's Name		Class Teacher	
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email (senior classes). 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 Name (print)			
Parent Signature		Date:	