Stranmillis Primary School

E-Safety Policy

Updated: January 2023

1. Rationale

The rapidly changing nature of the Internet and new technologies means that eSafety is an ever-growing and changing area of interest and concern. At Stranmillis Primary School, the staff, governors and parents have a duty of care to enable pupils to use online systems safely. This policy highlights the responsibility of the staff, governors and parents to mitigate risk through reasonable planning and actions. It covers not only Internet technologies, but also electronic communications via other mobile devices. This policy reflects the guidance in DENI Circular 2007/1 *'Acceptable Use of the Internet and Digital Technologies in Schools'*, DENI Circular 2011/22 *'Internet Safety'*, DENI Circular 2016/26 'Effective Educational Uses of Mobile Digital Devices', DENI Circular 2013/25 *'eSafety Guidance'* and DENI Circular 2016/27 *'Online Safety'*.

Aims: What is eSafety?

1. eSafety is short for electronic safety.
2. eSafety in the school context is concerned with safeguarding children and young people in the digital world, with emphasis on learning to understand and use technologies in a positive way. It is less about restriction and focusses on the risks, as well as the benefits, so that the users feel confident online. Furthermore, eSafety is concerned with supporting pupils to develop safer online behaviours, both in and out of school. It also helps pupils recognise unsafe situations and how to respond to risks appropriately.

Roles and Responsibilities

Our eSafety committee.

Mrs Linda Wilson (Principal)

Dr Maureen Thatcher (eSafety Nominated Rep on Board of Governors)

Mrs Jenny McKay(KS 2 Co-ordinator, eSafety Co-ordinator, ICT Co-ordinator and SLT)

Mrs Orlaith McLaughlin (Designated Child Protection Teacher and SLT)

Mr Terry McCorry School Support Northern Ireland

Primary 7 School Council Representatives

The policy 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 two Internet services in its infrastructure. Internet access is filtered for all users.

1.1. C2k is responsible for the provision of ICT managed services 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. Forcepoint (formally Websense) filtering is in place for Internet access. Customised filtering is managed by Mr McCrory and Mr Arneill (ICT Co-ordinator) and approved by the eSafety committee. Internet use is monitored, and access to the Internet via the C2k Education Network is fully auditable and reports are available to the school Principal. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. Staff and pupils accessing the Internet will be required to authenticate using their C2k username and password.

1.2. The school installed a BT Internet line in 2013 to enable a consignment of iPads to access online Internet services. We have taken appropriate measures, including carrying out a risk assessment, to safeguard this equipment against security breaches. The school works with an Information Technology and Outsourcing company (School Support Northern Ireland) and they installed a Draytek router with cyen filter. In addition, pupils accessing the Internet on iPads must do so using the K9 browser, which is an internet filter App.

Making use of the Internet in School

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. At Stranmillis, we equip our students with all the necessary ICT skills that they will need to help them progress confidently into a professional working environment. Students will be taught to be critically aware of materials they read and how to validate information. They use age-appropriate tools to search for information online. Pupils are made aware of copyright and plagiarism and encouraged to validate the accuracy of information which they research.

Acceptable use of the Internet

1. Code of Practice: The school has a Pupil Code of Practice (Appendix 1) and a Staff Code of Practice (Appendix 2) containing eSafety rules which make explicit to all users what is safe and acceptable and what is not. This Code of Practice will be issued to each pupil at the start

of each school year and consent must be obtained before the pupil can access the Internet. The Staff Code of Practice is agreed by all members of staff and is signed at the beginning of the new school year.

2. Pupil Sanctions: Minor school related incidents (whether in school or out of school) will be dealt with by Mrs McKay and the School Leadership Team. Mrs McKay will keep a record of all reports. This may result in parents being informed and a temporary ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's Safeguarding and Child Protection Policy. Users will understand their responsibilities to report eSafety incidents. Incident reports will be logged by Mrs Wilson for future auditing and monitoring, to allow the school to review and update eSafety policy and practices. Pupils are aware that any misuse of mobile phones/websites/email/social media should be reported to a member of staff immediately.

Internet Safety Awareness

1. Education of Pupils: Pupils are educated in the safe and effective use of the Internet and eSafety guidelines are displayed prominently around the school. A planned eSafety education programme for Years 1-7 takes place through assemblies, discrete lessons and wider curriculum opportunities. The Pupil Code of Practice is discussed at the beginning of each school year and referred to on other occasions as appropriate. Primary 7 School Council Representatives sit on the eSafety Committee. A list of Guidelines for online safety is shared with all staff, who in turn, share the information with their class (Appendix 3).

2. Professional Development for Teachers: Teachers are the first line of defence in eSafety. Their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. eSafety training is an essential element of staff induction and on-going Professional Development. It is linked with Safeguarding training at the beginning of every school year and it is compulsory for all staff to attend.

   The ICT Co-ordinator keeps informed and updated on issues relating to eSafety. Staff have been advised of available resources to facilitate the teaching of eSafety. These include:

   - **www.thinkuknow.co.uk**
   - **www.childnet.com**
   - **https://projectevolve.co.uk**

3. Governors: Mrs Wilson keeps governors updated on eSafety issues. The Board of Governors has appointed Dr Maureen Thatcher as their representative on the school eSafety Committee.

4. Parents, Carers and the Community: Parents and carers are encouraged to discuss the Pupil Code of Practice with their children before signing the acceptable use of the internet agreement. The eSafety Policy is available on the school website. The school organises sessions on eSafety which may be delivered by a member of staff or outside agency. For example, the PSNI or NSPCC. Parents are informed how to highlight issues, as detailed in the Bullying and Safeguarding policies. Parents are informed of the school's complaints policy which is on the website.
5. Community use of school ICT resources: Anyone using the school's ICT resources must agree to the Staff Code of Practice Policy before participating, and only access pre-selected and appropriate websites.
6. ICT/esafety co-ordinator, Designated teacher and School staff use Safer schools App to keep update with current safety issues and developments

Health and Safety

1. Risk Assessments: Life in the 21st century presents dangers including violence, racism and exploitation, from which pupils need to be reasonably protected. The school endeavours to help the children to become "Internet-wise" and responsible "digital citizens". We have considered all new technologies wisely, to ensure that we are fully aware of, and can mitigate against, the potential risks involved with their use. Mr McCorry and Mrs McKay complete an annual risk assessment for the use of the BT Internet line.
2. Cyber Bullying: Staff are made 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 the school's overall Anti-Bullying Policy. Cyber Bullying can take many different forms and guises including:
    - Email – nasty or abusive emails including viruses or inappropriate content.
    - Instant Messaging (IM) and Chat Rooms – transmitting, threatening or abusive messages.
    - Social Networking Sites – posting or publication of nasty of upsetting comments.
    - Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
    - Mobile Devices – abusive texts, video or photo messages, including sexting (where someone is encouraged to share intimate photographs or videos of themselves which are subsequently transmitted to other people).
    - Abusing personal information – posting of photographs, personal information, fake comments and blogs, or pretending to be someone online without permission.

Pupils will be reminded that cyber bullying can constitute a criminal offence. They are encouraged to report incidents to their parents and the school. If appropriate, the PSNI may be informed to ensure the matter is properly addressed and the behaviour ceases. The school will keep records in accordance with our Anti-Bullying and eSafety policies.

3. Pupil use of Mobile Phones and Personal Devices: Pupils are not permitted to bring mobile phones or personal devices to school. In exceptional circumstances, they must inform their class teacher and the device must then be switched off and kept in a locked cupboard until the end of the school day. Pupils who breach this rule may have their device confiscated. The school accepts no liability for the loss or damage of any electronic device which is in the pupil's possession during the school day.
4. Staff use of Mobile Phones and Personal Devices: Staff should not use their own personal devices to contact pupils or parents in or out of school time. They are not permitted to take photographs or videos of pupils with their own devices. This should be done using school equipment. The school expects staff to lead by example when using personal devices. Mobile phones should be switched off or on 'silent' during working hours.
5. Digital and Video Images: Parental permission is gained for the publication of personal images for display, use on the school website or use by outside media. Digital and video images are stored securely on the school network in the 'Staff' folder.
6. Email Security: Staff and pupils should only use their C2k email accounts for school purposes. It is strongly advised that staff should not use home email accounts for school business. The C2k Education Network filtering solution provides security and protection to C2k email accounts, ensuring that incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.
7. Personal Data: The school ensures all staff know and understand their obligations under the Data Protection Act (1998) and comply with these to ensure the safe keeping of personal data, minimising the risk of loss or misuse of personal data.
8. Passwords: Pupils and staff should only log on under their own username and password. Staff and pupils shouldn't share their passwords.

Published Content (Twitter) and the School Website

The school website www.stranmillisprimary.org.uk and Twitter is used to celebrate pupil's work, promote the school and provide information. The following rules apply:

- The point of contact on the website is the school address, school email and telephone number.

- Staff or pupils' home information will not be published.
- Online photographs which include pupils will be selected carefully in line with parental consent.
- Pupils' full names will not be used in association with photographs.
- Mr Arneill, Mrs Wilson and KS co-ordinators will take editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Social Media

C2K Forcepoint Internet filtering filters out social networking sites and blocks attempts to circumvent their filters, leaving it relatively safe in the school environment. Concern, in relation to inappropriate activities, tends to emanate from use outside of school. (See Anti-Bullying and Safeguarding Policies for reporting procedures) We make staff, pupils and parents aware of the risks associated with social media and encourage responsible use outside of school.

Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole, and takes the protection of school data and personal protection very seriously. This means protecting the school network against viruses, hackers and other external security threats. The security of the school information systems will be reviewed by C2K and virus protection software is updated automatically.

Monitoring and Self Evaluation

ESafety is evaluated in the overall ICT and Safeguarding Child Protection Policy reviews. Pupils offer a voice through their representation on the E-Safety Committee. The 360° Safe eSafety Self Review Tool has enabled the school to identify areas for development. Monitoring records of eSafety incidents are presented to the Governors. This policy will be reviewed and amended in light of evidence provided by monitoring, updated technologies or new DE Guidance.

Appendix 1

Acceptable Use of the Internet Agreement: Pupil

Acceptable Use of the Internet Agreement – Pupil and Parental Guidance

Parents/Guardians should read through this document with their children. Internet access will only be granted after this document is signed and returned to school.

- ✓ I will only use ICT, including the Internet, email, iPad, digital camera, mobile technologies etc. for school purposes.
- ✓ I know that my use of ICT is monitored and that my parent/guardian will be contacted if a member of staff is concerned about my e-Safety.
- ✓ I will log onto the My School Platform with my own username and password.
- ✓ I will not share my username or password with other people.
- ✓ I will only access the Internet when given permission by a member of staff.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number of home address. I will not arrange to meet someone through an online activity, unless this is part of a school project and a responsible adult comes with me.
- ✓ I will only open/delete my own documents and folders.
- ✓ I am not permitted to use any form of social media when in school.
- ✓ I understand that I am not permitted to post photographs or videos from a school activity on social media.
- ✓ I will ensure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will always reference the source of any information gained from the Internet.
- ✓ I am not permitted to bring or use a mobile/personal device when in school.
- ✓ The defintion of a personal/mobile device: any device, owned by an individual, with the capability to process, store or transmit information independently. This includes, but is not limited to, mobile phones, smartphones, smartwatches tablets, PCs, laptops and cameras.

Pupil's Name		Class Teacher	
I accept the rules and guidelines detailed above, and I will endeavour to be a responsible and safe user of ICT at Stranmillis Primary School.			
Pupil's Signature		Date	
I have discussed the guidelines and rules detailed above, and I give permission for my child to use ICT at Stranmillis Primary School.			
Parent/Guardian		Signature	

Photographs at School Events

Parents are permitted to take photographs of their children participating in events such as Sports Day, School Plays etc. In order for this practice to continue we need parents to undertake that any photographs / videos that may be taken will be for family use and will not be shared on social media etc.

In keeping with this policy any photographs that we take at school events will be of our own children and will not be shared on social media etc.			
Parent/Guardian		Signature	

Appendix 2

Acceptable Use of the Internet Agreement: Staff

Acceptable Use of the Internet Agreement – Staff Guidance

- ✓ I will only use ICT, including the Internet, email, iPad, digital camera, mobile technologies etc. for school purposes. All Internet activity, and electronic communications with pupils and staff, should be appropriate to staff professional activity or the pupils' education.

- ✓ I will comply with the ICT system security and not disclose or share passwords provided to me by the school or other related authorities.

- ✓ I am responsible for all email sent and for contacts made that may result in email being received. I will use the approved c2k secure email system for school business.

- ✓ I will not give out personal details e.g. mobile phone number and personal email address, to pupils.

- ✓ Copyright of materials must be respected and I will always reference the source of any information gained from the Internet.

- ✓ I will not use social media on the c2k network. Neither will I post images or videos from a school activity on social media.

- ✓ I understand that any personal mobile device I have in school must be kept on silent during school hours.

- ✓ Photographs and videos of pupils and staff must only be taken using a school digital camera or iPad. They can only be stored and used for professional purposes in line with school policy and with written consent of a parent or guardian (Data Collection sheet at the start of each new school year). Photographs or videos will not be distributed outside the school network without the permission of parent/guardian, staff member or Principal.

- ✓ I will not install any hardware or software on the c2k system without the permission of Mr Arneill.

- ✓ 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. I will report any concerns, or misuse of ICT by pupils or staff, to Mrs McKay.

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school.		
Staff member:	Signature:	Date:

Appendix 3

Online Safety Guidelines for pupils at SPS

CONDUCT

- Only use the Internet when we have permission from an adult.
- Always be polite and friendly. Don't post comments or send an email that is nasty or inappropriate – remember it is written down and can be printed out.
- If you wouldn't say it in real life, don't say it online.
- Information you put online leaves a permanent "digital footprint".
- Don't make your email address your full name or date of birth.
- Try to create strong and secure passwords.
- Ask your parent/guardian to set appropriate privacy settings for any Apps you are using.
- Don't purchase anything online without permission – including in-App purchases.

CONTENT

- Immediately close any close any page we are not sure about.
- Don't deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my parent or guardian immediately. (Or teacher if in school)
- Only use apps or websites approved by my parent/guardian. (Or teacher if in school)
- Always respect, and adhere to, the age restrictions on games, websites and Apps.

CONTACT

- Meeting someone you have been in touch with online can be dangerous. NEVER do this.
- Don't make friends with someone online, if you haven't met in that person in real life.
- Don't open messages, emails, pictures or texts from people you don't know.
- Don't share person information online.
- Only email people an adult has approved.

TELL

- You must tell a parent, carer or trusted adult if someone or something makes you feel uncomfortable, worried, angry, hurt or fearful, or if someone you know is being bullied online.