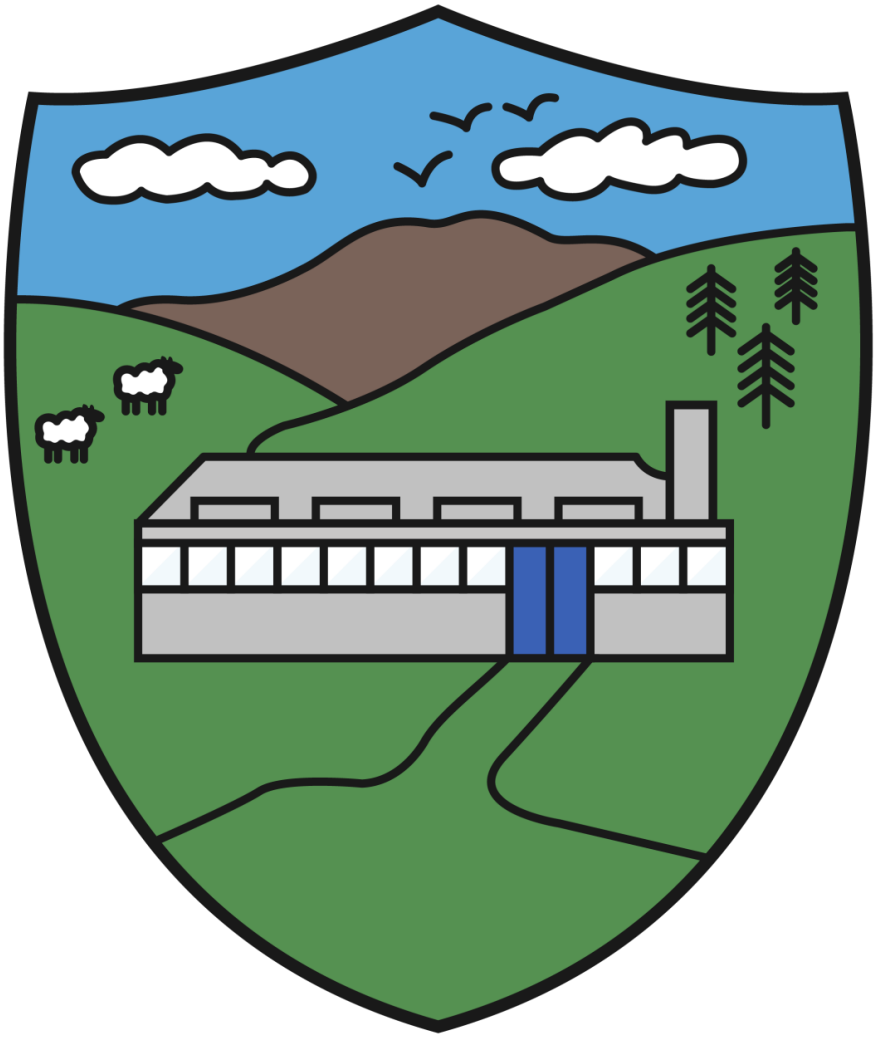
E-Safety Policy

St. Paul's P.S



This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools.

The above circular 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."

It also complies with the more recent circulars on E-Safety guidance; 2011/22, 2013/25, 2015/21 and 2016/25.

This document sets out the policy and practices for the safe and effective use of the Internet and other digital technologies in St. Paul's Primary School.

UNCRC:
Article 16
Every child has the right to privacy. The law should protect the child's private, family and home life.

Article 17
Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

Introduction
Information and Communications Technology (ICT) covers a wide range of resources including the Internet and other digital technologies. Used effectively and appropriately, these powerful digital technologies have the potential to enhance and transform teaching and learning by giving teachers and children access to a global network of educational resources.

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 the Internet and digital technologies.

In St. Paul's Primary School, we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach pupils 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 a unique and exciting resource. 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 online who may wish to harm them.
Some adults use social networks, gaming 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
- 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
- That 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.

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.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave online and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

E-Safety Information for Parents/Carers

- The school will communicate relevant E-Safety information through curriculum evenings, newsletters and the school website.
- Parents should remember that it is important to promote E-Safety in the home and to monitor Internet use.
- Keep the computer in a communal area of the home.
- Monitor the use of all digital technologies, e.g. gaming stations and portable technologies such as tablets and smart phones.
- Monitor online time and be aware of excessive hours spent on the Internet.
- Take an interest in what your child is doing. Discuss with your child what he/she is seeing and using on the Internet.
- Advise your child to take care and to use the Internet in a sensible and responsible manner. Know the SMART Tips. (Appendix 1)
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how your child should respond to unsuitable materials or requests.
- Remind your child never to give out personal information online.
- Remind your child that people on line may not be who they say they are.
- Be vigilant. Ensure that your child does not arrange to meet someone they meet online.
- Be aware that your child may be using the Internet in places other than in your own home or at school and that this internet use may not be filtered or supervised.
- Monitor your child's use of mobile phone Apps for social media.
- Parents/carers are asked to read through and sign their child's Acceptable Use Agreement. (Appendix 2)
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website. (Appendix 3)

Internet Use

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety in relation to the use of digital technologies both inside and outside of school, as referenced in the annual ICT Action Plan.

- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them.

- Use of the Internet must be a planned activity, and although school Internet access is filtered through the C2k managed service, all pupil use of the Internet, including the use of iPads, must be supervised by an adult.

- Use of digital downloads, e.g.YouTube clips, for educational purposes must be viewed in advance of lessons to ensure appropriate content.

- Connection of mobile phones or personal computers to the school's wireless network is not permitted.

E-mail

- Pupils may only use C2k e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive e-mail or an e-mail from an unknown source.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Social Networking

- Pupils and parents should remember that the use of social network sites is inappropriate for primary aged pupils.

- The school C2k system will block pupil access to social networking sites.

- Parents who choose to allow their child to engage in social networking should closely supervise all online activity.

- School staff will not engage with pupils on these sites.

Mobile Technologies

- The use of portable media such as memory sticks and external hard drives should only be used to transport school related material.

- Staff should not store pupils' personal data or photographs on memory sticks / mobile phones.

- Pupils should not bring mobile phones to school.

- Written permission from a parent/carer must be obtained before a device is brought into school with an appropriate reason.

- Devices must be switched off during school hours and if travelling on the bus.

- Pupils who use their own mobile device in school or on the bus will be sanctioned appropriately.

- Staff should not use mobile phones for personal use during teaching sessions. The use of these devices at other times should be discreet.

- iPads will only be used under the direction of a member of staff for a particular educational purpose.

Remote Lessons and Homework Activities

Resources about keeping children safe online have been shared with parents on the school website. Staff may set work for pupils on Seesaw, Dojo or Google Classroom. When delivering live lessons, staff and pupils will follow guidance issued regarding appropriate behaviour on live lessons. Staff will not interact with individual children in any live lessons. A child may be invited to remain online to work with the teacher after all other children have left the session.

If interacting with other children or staff online, children should always be kind and respectful to each other and respectful and obedient to staff. Any inappropriate comments to staff online, via email, or any other platform will be taken very seriously. This is also the case for any online bullying towards other pupils or peer-on-peer abuse that is disclosed to the school during this time.

Teachers and parents may communicate with each other for school business using the private message facility on the communication platform. Group information from the teachers can be posted on the stream.

Communication between staff will be carried out via WhatsApp or e-mail in line with acceptable protocol, as outlined in the Staff Code of Conduct Policy.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. 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 circumstance.

- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' names will not be attached to any photographs on the school website.
- Pupils' work can only be published by outside agencies if parental permission is given.

Authorising Internet Access

- Pupils must sign up to the Acceptable Use Agreement and abide by the school's E-Safety rules.

- All parents will be asked to sign their child's Acceptable Use Agreement giving consent for their child to use the Internet in school.

- All staff must sign the Acceptable Use Agreement for Staff before using any school ICT resource. (Appendix 4)

Handling E-Safety Concerns

- Concerns regarding the use of the Internet/digital technology (deliberate or inadvertent) will be recorded on an E-Safety incident log and a record of each incident will be passed on to Mr. Geoghegan. If the concern is of a child protection nature, Mr Geoghegan will inform Mrs. Truesdale (DT).

- Any complaint about staff misuse must be referred to Mr. Geoghegan.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Staff Development regarding E-Safety will be an integral element of our annual child protection training.

Communicating the Policy

Keeping Pupils Aware of the E-Safety Policy

- E-Safety rules will be discussed with the pupils at the beginning of September each year and will be re-visited at the beginning of Term 2 and Term 3.
  Specific lessons will be planned and taught throughout the year.
  Further reinforcement lessons will be taught should the need arise.
  Particular focus will be placed of E-Safety with a "Safer Internet Day" at the beginning of ICT Week.

- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety Policy

- All staff will agree to the school's E-Safety Policy. The policy will be re-visited on an annual basis as part of the school's Child Protection training programme.

- 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.

- All staff must sign the Acceptable Use Agreement for C2k Laptops before using this resource annually.

- All staff must sign the Acceptable Use Agreement for school iPads before using this resource annually.

Parents and the E-Safety Policy

- The school's E-Safety Policy will be available for all parents to read on the school website. Paper copies will be available on request.

Monitoring and Review

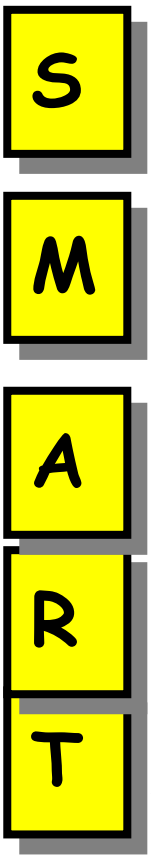
This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually.

Appendix 1

Safety Rules for Children

Follow These SMART TIPS



Secret - Always keep your name, address, mobile phone number and password private.

Meeting - Make sure you tell your parent or teacher if someone wants to talk to you online.

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.

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

Appendix 2

St. Paul's Primary School

Rules for Responsible Internet Use

The school has installed computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

- I will not access other people's files;
- I will only use the computers for school work and homework;
- I will not bring in memory pens/sticks from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail people I know, or people that my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Myself and my parents/guardian have read the rules. I will abide by the rules.

Pupil's Name: _____

Pupil's Signature: _____

I have discussed the above rules of use with my child.

Parent's/Guardian's Name: _____

Parent's/Guardian's Signature: _____

Appendix 3

St. Paul's Primary School

Acceptable Internet Use Statement for Staff

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties -the pupils, 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 using or requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to Mr Geoghegan.

- All Internet activity should be appropriate to staff professional activity or the pupil's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail 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 inappropriate materials such as pornographic, racist or offensive material is forbidden.

Name: _____

Signed: _____Date: _____

Appendix 4

St. Paul's Primary School

Acceptable Use Policy for School iPads

This policy should be signed by any member of staff who will take an iPad away from the school.

I understand that I am the *nominated member of staff* for this iPad, and I agree that:

Ownership of this iPad rests with the school, and that I may retain it for school use while in the employment of this school.

Use of the iPad, both in and outside school, is to be for school use only.

Logon and downloads to the iPads are only possible with the valid username and password and this should not be changed without consent.

The facility to install applications will be the responsibility of the ICT co-ordinator.

The iPad should be connected to the internet at least once a fortnight to scan and update applications.

The iPad may be used outside school for Internet use with any Internet Services Provider (ISP) e.g. BT wifi.
It is the responsibility of iPad users to ensure that confidential information is not saved to the iPad.

The iPad should not be given, lent or used by anyone other than the nominated member of staff when outside school.

The iPad should always be kept in the case to reduce the chance of damage.

The iPad must be returned to school if the nominated member of staff ceases employment with the school.

Staff Signature: _____

Date: _____