



Online Safety Policy
And
Acceptable Use Agreement

2023

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based 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
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile 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. Francis' Primary School*** we understand the responsibility to educate our pupils in Online Safety issues. We aim to teach the 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. 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.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details or
- That they should never meet alone anyone contacted via the Internet, and
- 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.

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.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

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 on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

As Online 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 UICT Co-ordinator to keep abreast of current online safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The UICT Co-ordinator has responsibility for leading and monitoring the implementation of online safety throughout the school.

The Principal/ICT Co-ordinator update Senior Management and Governors with regard to online safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice. The online safety governor will be kept informed regularly about online safety in the school by Miss Mc Morrow, ICT co-ordinator.

Writing and Reviewing the Online Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, 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 and Anti-bullying.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The Online Safety Policy and its implementation will be reviewed annually.

Online Safety Skills' Development for Staff

- All staff receives regular information and training on Online Safety issues through the co-ordinator at staff meetings, specific online safety training and UICT team meetings.
- All staff has been made aware of individual responsibilities relating to the safeguarding of children within the context of Online 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 incorporates Online Safety activities and awareness using the Commonsense Media Digital Literacy schemes of work and other relevant resources.

Online Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign their child's Acceptable Use Agreement.
- 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, school Facebook page or Home/School Digital Portfolio or Communication Apps such as Seesaw.
- The school website contains useful information and links to Online Safety sites.
- The school will communicate relevant online safety information through curriculum evenings, monthly newsletters, the school website page and the school text system.

Parents should remember that it is important to promote online Safety in the home and to monitor Internet use.

- 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.
- 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:

- The school will plan and provide opportunities within a range of curriculum areas to teach Online Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also 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 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.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- 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.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system or Google Drive Accounts.
- 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.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

- 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 bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Mobile Technologies:

- The use of portable media 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 / mobile phones
- Pupils are not allowed to use personal mobile devices/phones (in school) during class. Mobile phones must be kept in pupils' schoolbags, turned off until they leave the school premises.
- Staff should not use personal mobile phones during designated teaching sessions.

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 or carers will be obtained before photographs of pupils are published on the school website, Facebook page or Home/School Communication Apps such as Seesaw. 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' names will not be attached to any photographs on the school website.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

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 Online Safety rules.
- Access to the Internet will be supervised.
- All parents will be asked to sign their child's Acceptable Use Agreement giving consent for their child to use the Internet in school by following the school's Online Safety rules and within the constraints detailed in the school's Online 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 to the C2K System.
- All staff and pupils are provided with individual login username and password to their Google Drive Accounts.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff is aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling Online Safety Complaints:

- Complaints of Internet misuse will be recorded on an Online Safety incident log and a record of each incident will be passed onto Mrs Mc Stravick/Miss Rice.
- Any complaint about staff misuse must be referred to the Miss O'Dowd.
- 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.

Communicating the Policy:

Introducing the Online Safety Policy to pupils

- Online Safety rules will be discussed with the pupils at the start of each year. 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.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the Online-Safety Policy:

- All staff can access the School Online Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and 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.

Parents and the Online-Safety Policy:

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

Online Safety and Child Protection

- The school Internet access is filtered through the C2K managed service using a Websense filtering solution.

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.

The policy will be reviewed in June 2024 by Mrs Mc Stravick ICT co-ordinator.

ALWAYS BE SAFE- FOLLOW THE SMART RULES!

P4-P7

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!



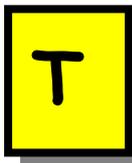
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



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.

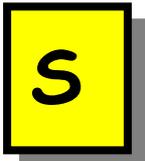
SMART Tips from: – Helping your parents be cool about the Internet,
produced by: Northern Area Child Protection Committees

ALWAYS BE SAFE- FOLLOW THE SMART RULES!

P3

Safety Rules for Children

Follow These SMART TIPS



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



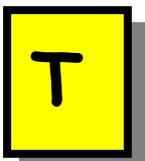
Make sure you tell your parent or teacher if someone wants to talk to you when you are online.



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

P5 – P7

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 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 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/cares will be informed.

Signed by Child:	_____
Signed by Parent/Guardian:	_____
Date:	_____

P3 and P4

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 which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- 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 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/cares will be informed.

Signed by Child:	_____
Signed by Parent/Guardian:	_____
Date:	_____

ST.FRANCIS’ PRIMARY SCHOOL

Acceptable Use Agreement

For staff and visitors

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 Internet Access Policy has been drawn up to protect all parties – the students, 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.

- All Internet activity should be appropriate to staff professional activity or the pupils' 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 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 inappropriate materials such as pornographic, racist or offensive material is forbidden

Name		
Date		Signed

St.Francis' Primary School Online Safety Incident Log

Time	
Date	
Where did the incident occur	
Name of person reporting the incident	
Who was involved in the incident	
Type of incident	<input type="checkbox"/> online bullying or harassment (cyberbullying) <input type="checkbox"/> sexting (self-taken indecent imagery) <input type="checkbox"/> deliberately bypassing security or access <input type="checkbox"/> hacking (unauthorised entry to computer system) or spreading a computer virus <input type="checkbox"/> racist, sexist, homophobic religious hate material <input type="checkbox"/> terrorist material <input type="checkbox"/> other (please specify) _____
Description of incident	
Nature of incident	<input type="checkbox"/> deliberate access <input type="checkbox"/> accidental access
Did the incident involve material being	<input type="checkbox"/> created <input type="checkbox"/> viewed <input type="checkbox"/> printed <input type="checkbox"/> shown to other <input type="checkbox"/> transmitted to others <input type="checkbox"/> distributed
Action taken	<input type="checkbox"/> incident reported to member of staff (specify) _____ <input type="checkbox"/> child's parents informed <input type="checkbox"/> disciplinary action taken <input type="checkbox"/> child/young person debriefed

Please make a copy of this e safety incident log for Mrs McStravick.
Keep the original copy in your Pastoral Care File.

Online Safety Policy taken guidance of DENI Circular 2016/27

Mrs Mc Stravick June 2023