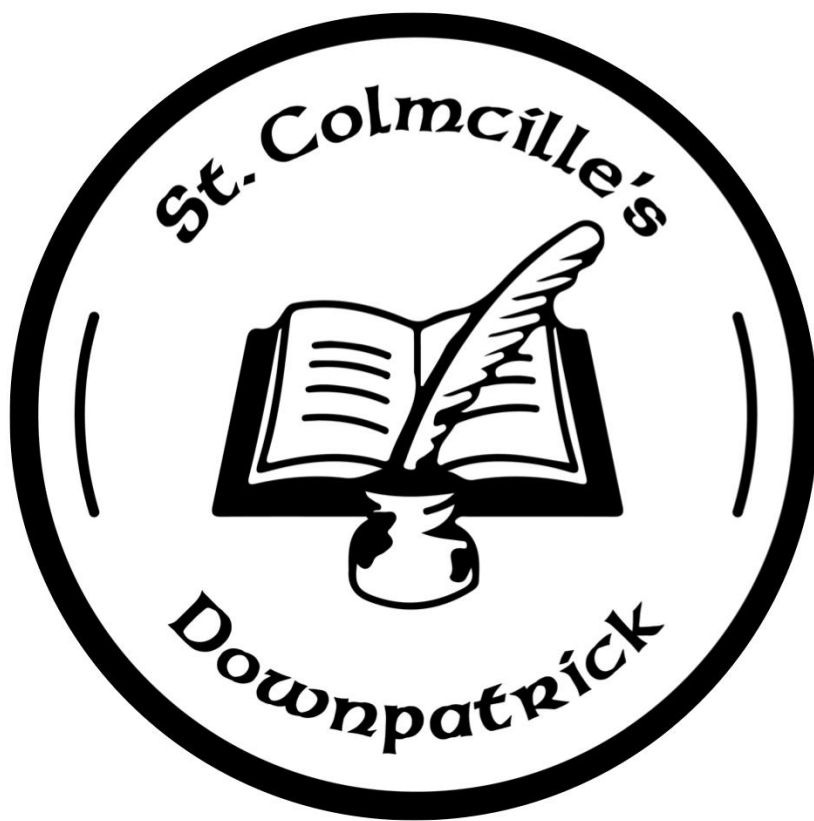


Digital Safety & Acceptable Use Policies



Rationale

“The school’s actions on and governance of online safety must be reflected clearly within the school’s safeguarding arrangements and Online Safety Policy. Safeguarding and promoting pupils’ welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities.”

DENI Online Safety Guidance, Circular number 2016/27

It is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Digital Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and other wireless technology.

The school must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The Digital Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. The internet technologies children and young people are currently using, both inside and outside of the classroom, include but are not limited to:

- Websites/Apps
- 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 Colmcille's Primary School, we understand the responsibility to educate our pupils about digital 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.

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 and potential risks for the school can be categorised as the Contact, Content and Conduct of activity.

1. Contact

- Inappropriate communication / contact with others, including strangers.
- The risk of being subject to grooming by those with whom they may make contact on the internet.
- Cyber-bullying.
- Unauthorised access to / loss of / sharing of personal information.

2. Content

- Access to illegal, harmful or inappropriate images or other content.
- Access to unsuitable video / online games.

- An inability to evaluate the quality, accuracy and relevance of information on the internet.

3. Conduct

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The sharing/ distribution of personal images without an individual's consent or knowledge.

➤ Potential Contact

Children may come into contact with someone online 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 people they encounter through the internet.
- That they should never give out personal details.
- That they should never arrange to meet anyone contacted via the internet.
- That once they publish information it can be disseminated with ease and cannot be destroyed.

➤ Inappropriate Content

Throughout 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 financial 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 online and to discuss problems. There are no totally effective solutions to problems of internet safety. Teachers, pupils, parents and carers must be vigilant.

Roles and Responsibilities

As digital safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Coordinator and ICT Team to keep abreast of current digital safety issues and guidance through relevant organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Coordinator will ensure that all staff are aware of the procedures that need to be followed in the event of a digital safety incident taking place and provide training and advice for staff. The ICT Coordinator and Principal will also liaise with C2k/EdIS, EA and DENI regarding any digital safety developments.

The ICT Coordinator has responsibility for leading and monitoring the implementation of digital safety throughout the school.

The Principal/ ICT Coordinator update Senior Management and Governors regarding digital safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Designated/ Deputy Designated Child Protection Officer

The Designated Child Protection Officer and their deputy will be trained in digital safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying.

Managing the Network

The ICT Team will monitor that C2k/EdIS online safety measures, as recommended by DENI, are working efficiently within the school. They will ensure that:

- C2k/EdIS systems operates with robust filtering and security software.
- Monitoring reports of the use of the C2k/EdIS and BT Business networks are available on request.
- School devices, infrastructure and individual workstations are protected with latest updates.
- School meets required digital safety technical requirements.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering and security group policies are applied and that its implementation is not the sole responsibility of any single person.
- They keep up to date with digital safety technical information in order to effectively carry out their digital safety role and to inform and update others as relevant.
- The administrator passwords for school systems, used by the network managers, must always be available to the Principal and kept in a secure place.

Writing and Reviewing the Digital Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

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

Digital Safety Skill Development for Staff

- All staff receive regular information and training on digital safety issues from the ICT Coordinator/ICT Team at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of digital safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff and visitors receive information on the school's Acceptable Use Agreement as part of their induction or welcome to the school.
- All staff are encouraged to incorporate digital safety activities and awareness within their lessons.

Digital Safety Information for Parents/Carers

- Parents/carers are asked to read through and agree to the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used on the school website, social media channels and those of our partner organisations.
- The school will communicate relevant digital safety information through newsletters, the school website and social media channels.

Parents/carers should remember that it is important to promote digital safety in the home and to monitor internet use.

- Keep the computer or devices 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 online 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 platforms and apps 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 online may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- 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.

CCTV

The school has CCTV as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission, except if disclosed to the Police as part of a criminal investigation.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach digital 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 digital 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's wired and wireless network is filtered through C2k/EdIS.
- There is also third-party Wi-Fi provided by BT Business for the purpose of operating the school telephone system. The BT Business Wi-Fi network is filtered and is solely for use of the principal and key members of office staff, to facilitate their school related duties. It is not available for use by pupils or visitors.
- 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 Digital Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. **SMART** tips are discussed and displayed in class.

E-mail:

- Pupils may only use C2k/EdIS e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- The forwarding of chain mail/SPAM 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/EdIS system will block access to social networking sites.
- The Principal and School PR Team will have access to social networking sites, to allow the management and operation of school's social media channels.
- Pupils and parents/carers will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils may still use them. They will be advised never to give out personal details of any kind, which may identify them or their location.
- The school will provide training in the appropriate use of social networking/ for teaching and learning purposes.

- Training will include acceptable use, social media risks, checking of settings, data protection, reporting issues and legal risks.
- 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.
- Staff should report any incidents of cyber-bullying to the school.
- Further information is provided to staff during in service training.
- School staff will not engage with children on 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.
- The use of cloud-based storage, e.g. OneDrive, is encouraged to minimise risk.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile devices/ phones (in school) or on school trips, unless specific permission is given by school staff.
- Staff should not use personal mobile phones during designated teaching sessions or when undertaking supervision, unless in the event of an emergency.
- Pupils must not use smartwatches as a communication device, or to record audio, video or images on the school site or while on a school trip or activity. Use of smartwatches in this way will result in the device not being allowed in school.

Managing Video-conferencing:

- Videoconferencing will be via the C2k/EdIS network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.
- Weekly assemblies will be held via the Zoom platform, this will be organised via a designated Zoom account and links will be sent only to staff.
- Any video-conferencing involving pupils outside of the weekly assembly will be held via Microsoft Teams using the relevant C2k/EdIS accounts.

Publishing Pupils' Images and Work

- Permission from parents/guardians will be obtained before photographs and videos of pupils are published on the school website, social media channels and those of our partner organisations. This consent 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.
- Photographs/videos that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school website social media channels and those of our partner organisations, particularly in association with photographs and videos, except where required by publication/editorial guidelines e.g. in local newspapers.
- Photographs/videos of individual pupils will be limited, unless required for teaching, learning or assessment. Group pictures will be encouraged.

GDPR

The school is GDPR compliant and staff are regularly reminded of their responsibilities. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media, it is advisable that:

- The device is password protected.
- The device offers approved virus and malware checking software.
- The data is securely deleted from the device, in line with school policy, once it has been transferred or its use is complete.

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 digital safety rules. **These Digital Safety rules will also be displayed clearly in all rooms.**
- Access to the internet will be supervised.
- All parents will be asked to read and agree to the Acceptable Use Agreement for pupils giving consent for their child to use digital devices in school by following the school's digital safety rules and within the constraints detailed in the school's Digital Safety Policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using the school network or any school ICT resource.

Password Security

- Adult users are provided with an individual usernames and passwords for school systems, devices and school-provided platforms, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual 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 and school devices.
- Pupils are not permitted access to devices which are logged in to staff members' accounts.

Handling Digital Safety Complaints:

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Coordinator and recorded in the Digital Safety Incident Log.
- 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/carers will be informed of the complaints' procedure.

Cyber-Bullying

Cyber-bullying can take many different forms and guises including:

- Email- nasty or abusive emails which may include viruses or inappropriate content.
- Messaging Apps and Forums- 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 or platforms.
- Mobile Phones- examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information- may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Incidents of cyber-bullying will be dealt with in accordance with the school Anti-Bullying Policy.

Communicating the Policy

Introducing the Digital Safety Policy to Pupils

- Digital Safety rules will be displayed in all teaching/learning areas and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers throughout the year e.g. during PDMU lessons/ circle times/ Anti-Bullying Week/ Safer Internet Day .etc.
- Pupils will be informed that device, network and internet use will be monitored.

Staff and the Digital Safety Policy

- All staff will be given the Digital Safety Policy and its importance will be explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that device use, internet activity and emails can be monitored and traced to the individual user. Discretion and professional conduct are 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.

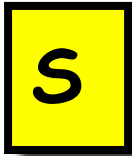
Monitoring and review

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

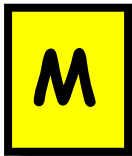
This policy will be reviewed annually.

Digital Safety Rules for Pupils

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!



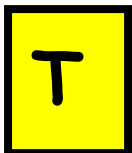
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



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.



St Colmcille's Primary School Acceptable Use Agreement for Pupils

Children should know that they are responsible for making Acceptable Use of the Internet. To use the school network and school devices, 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.

- When using school devices or school-provided platforms, I will only use my own usernames and passwords.
- I will keep my usernames and passwords private.
- I will not access other people's files or data without their permission.
- I will not change or delete other people's work, files or data.
- I will ask permission before entering any app or website, unless my teacher has already approved that site.
- I will use school devices and the internet for research and school purposes only.
- I will only send emails, messages or comments which my teacher has approved.
- I will make sure that the messages or comments that I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using school devices.
- When sending email or other communications, 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, forums or messaging services while using school computers or devices.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a staff member immediately.
- I understand that personal devices should not be brought into school and should never be connected to the school's network.
- I will not bring in memory sticks or portable 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 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 or author, in the documents I produce.

- I understand that if I deliberately break these rules, I could be stopped from using school devices and my parents/cares will be informed.

Agreement of Pupil		
As a school user of digital devices and the internet, I agree to follow the school rules on their use. I will use school network and devices in a responsible way and observe all the restrictions explained to me by my school.	Agree	Disagree
Agreement of Parent/Guardian		
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use school ICT devices and the internet, including email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials, platforms and services on the internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when using digital devices.	Agree	Disagree



St Colmcille's Primary School Acceptable Use Agreement for Staff

The school network and devices are made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Digital Safety 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 devices or system or to monitor any activity on them.

Staff should read this Acceptable Use Agreement and complete the form below.

- All activity using school devices and the school network should be appropriate to staff professional activity or the pupils' education.
- Access should only be made via authorised account logins and passwords, 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 the content of all emails 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 or spam is forbidden.
- As email 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 school network or devices to access inappropriate materials, information or content is forbidden.
- Use of school devices and the school network is monitored to ensure compliance and appropriate device deployment.

Name of Staff Member or Visitor:		
As a user of the school network and devices, I agree to follow the regulations stated above regarding their use and will use school network and devices in a responsible way.	Agree	Disagree