



**Acceptable
Usage Policy**

Introduction

Information and Communication Technologies (ICT) offer teachers and pupils educational tools and resources which extend their learning environment. Our current ICT resources include individual teacher laptops, 5 ProWise interactive touch screen boards, a computer suite with 15 Windows PCs and 30 Apple iPads (with 2 mobile charging cases).

When used to support the aims, principles and objectives of the Primary School Curriculum, these technology tools have the potential to augment and transform classroom teaching and learning. Learning may be with ICT, through ICT or about ICT.

Aim

The aim of this Acceptable Usage Policy is to ensure that pupils and teachers will benefit from teaching and learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and a privilege. Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions (as outlined below) will be imposed.

Pupils and teachers engage with the curriculum through ICT. in many ways, for example:

1. Using high quality interactive educational Internet provided activities/apps.
2. Using word processing packages which encourage the draft-edit-publish approach to creative and functional writing.
3. Engaging in Internet research in a wide range of curricular areas.
4. Staff using digital projectors and interactive white boards can access, prepare and use a wide range of materials and resources which are visually appealing and stimulate whole class discussion.
5. ICT equipment (such as the i-pads) can also be used under supervision for project work etc.
6. The school website (www.stmarysnscastlefinn.com) and Facebook page provides an opportunity for teachers and pupils to publish and celebrate activities and projects in which the school is involved.
7. The website also provides valuable communication for parents about the school and allows for input to policies etc.
8. It is envisaged that pupils will not only be consumers of ICT/digital technologies but also that they will be producers using ICT i.e. Book Creator, Seesaw etc.
9. ICT will be an integral tool to pupil self-assessment, peer assessment and teacher assessment.

Internet /World Wide Web

- Internet sessions will always be supervised by a teacher.
- All surfing should have a purpose. Search Engines sometimes provide too wide a focus leading to inappropriate sites.
- The Schools Broadband Network is filtered by NCTE.
- Downloading or uploading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- Pupils will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Pupils will report accidental accessing of inappropriate materials.
- Pupils will use the internet for educational purposes only.
- Pupils will acknowledge the source of their research.

- Pupils will never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies is not allowed.
- Pupils will be aware that any usage including distributing or receiving information, school related or personal may be monitored for unusual activity, security and /or network reasons.
- Time spent on special reward sites should be kept to a minimum.
- If an unacceptable site is accessed, it should be deleted immediately or monitor switched off and reported to the teacher / ICT co-ordinator. The ICT co-ordinator in St. Mary's National School is Mrs. Rachel Mc Cready.

Email

- Teachers will only communicate with parents/guardians through their designated school gmail account. These accounts are strictly for school use only.
- Pupils may only use approved school or class email accounts under supervision by or permission from a teacher.
- Pupils will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Pupils will not reveal their own or other people's personal details such as addresses, telephone numbers or pictures.
- Pupils will never arrange a face to face meeting with someone they only know through emails.
- Pupils will note that sending and receiving email attachments is subject to permission from their teachers.

Social Networking & Chat Rooms

Social networking or chat rooms may not be accessed in St. Mary's National School.

Mobile Phones

Mobile phones **are not permitted**. If a pupil brings a mobile phone into school, it will be confiscated and left in the principal's office. Upon request, the phone will be returned to the parent/guardian. No phones are allowed on school tours. In exceptional circumstances if a child requires their mobile phone after school, a letter of permission needs to be sent to the school explaining this. The phone will be switched off and kept in the school office until 3.p.m

School Website

- Our school website is www.stmarysnscastlefinn.com
- Information for the whole school community is posted on the website on a regular basis.
- The school website is evolving all the time and we hope to update it as much as possible. Children will be given the opportunity to publish projects, artwork, and school work on the school website with parental permission (Appendix 1).
- The publication of student work will be co-ordinated by the teacher and/or the ICT co-ordinator.
- Children will continue to own the copyright on any works published.
- The copying of such content is prohibited without express written permission from the relevant child and his/her parent(s)/guardian(s). Upon request, permission for reproduction will only be granted when a Reproduction Permission Letter (Appendix 2) is returned to the

relevant class teacher with both the child's and a parent/guardian's signatures on it.

- The school will endeavour to use digital photographs, audio or video clips focusing on group activities (rather than individual pupils).
- The school website will avoid publishing the first name and last name of individuals in a photograph. Personal pupil information including home address and contact details will be omitted from school web pages. Pupil /staff names will not be used to identify files on the website.

Consent

Parents should be aware that internet access is designed for educational purposes. Parents should also understand that the school cannot be held responsible if pupils access unsuitable websites as every reasonable precaution has been taken by the school to provide for online safety. Please contact the school in writing if you decide not to allow your child access to the internet as defined in this policy (Appendix 1). Specific consent for the use of digital images was requested on the enrolment form before commencing school at St. Mary's National School. Photographs/video may be used for souvenir DVD's or other school related presentations and promotions in the local media.

Internet Safety

Parents and teachers monitor usage and advise on pupil safety at all times. Advice on internet safety will be offered to parents, pupils and teachers on a yearly basis through an outside agency. Further advice is available on www.webwise.ie/www.donegalyouthservice.ie.

National Schools Broadband Service

St. Mary's National School Castlefinn uses the National Schools Broadband Service which automatically filters what we can see when we use the internet, blocking sites and content considered inappropriate. It also features the provision of the following centrally hosted services to further enhance internet safety and security.

- Secure email and other educational applications i.e. content filtering will block inappropriate email or web content.
- Online security services including firewall (prevents unauthorised access by outsiders to the school network), anti-virus software (programs or codes which can 'infect' a computer when attached to downloaded material) and spam (unsolicited emails) management.

Cyber bullying

Parents should be aware of potential cyberbullying by monitoring their children's usage at home. The Board of Management of St. Mary's National School promotes a 'social media free school' campaign annually. **Our Board of Management ask that pupils at the school do not have social media accounts as they are not the required age.** In recent years, it has come to our attention that children attending our school were using their networked devices – phones, tablets, laptops and x-boxes/playstations/nintendo switches inappropriately at home. Their unsupervised actions were causing distress for their peers and some difficulties were spilling over into the school. It is the school's reasonable request that pupils attending our school **should not** communicate inappropriately to or about each other using these networked devices. In school, teachers strictly monitor the allowed use of school technology ensuring that cyberbullying does not happen on our watch. At home or in the community, it is important that children are also supervised when on line. As already stated, primary school children should not have access to social networking sites. Ongoing education and

awareness is necessary for us all in these challenging times.

A parental e-safety guide is available at www.esafetykit.net or www.saferinternet.org Please encourage your children to be kinder to each other and to consider the feelings of others.

Sanctions

Misuse of the internet may result in disciplinary action including written warnings, withdrawal of access privileges and in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Ipads

- Ipad batteries are required to be fully charged every morning and be ready to use in school. It is the responsibility of each individual teacher to ensure that they are cleaned, charged and securely stored after each use.
- Memory space is limited. Academic content and apps takes precedence over personal files.
- Pupils are subject to individual teacher classroom management rules and should follow all instructions of their teacher in class.
- Pupils are not allowed to use any app which is unrelated to class work.
- Pupils are prohibited from deleting internet history unless given specific instruction by the class teacher.
- Pupils should take care not to leave their device on table edges or in any position where damage may occur.
- Any recording of a fellow pupil or staff member is expressly forbidden unless under teacher direction and supervision.
- Downloading/accessing social media sites on school ipads is prohibited.

Staff Devices

All staff laptops and desktops are encrypted and have two secure passwords. Staff have been advised to:

- Avoid bringing laptops home. If necessary, however, they should be stored out of sight in the boot whilst in transit and staff should never leave them in an unoccupied car overnight.
- All desktops and laptops should have encryption and passwords.
- Pupil information should not be stored on personal laptops.
- USB keys containing school information should be protected and kept at school.
- No personal USB keys should be inputted to school computers.
- Always switch off computers at the end of the day.
- Staff mobile phone use should be kept to a minimum (break times only) and during teaching time, available for emergency contact only.
- Staff should take good care of all ICT equipment in classrooms, powering them off each evening. Any difficulties should be reported to the principal/I.C.T co-ordinator.
- Food or liquids are not allowed near school laptops/computers.

School's Strategy

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the internet.

Teachers may support their pupils via online platforms such as email and Seesaw. Parents will be contacted by phone, email or Seesaw. In all instances, parental/guardian consent is given either by ticking consent on app, by response to email, or by providing the school with phone details. Sometimes parents/guardians will ask for teachers support with regard to their child's wellbeing or self-motivation, and teachers may get in touch with parent/guardian to facilitate same.

Parent and Pupil Zoom Call Guidelines

In order to create a safe environment for pupils and staff when taking part in Zoom calls, the following considerations must be observed:

- Zoom is only to be accessed by a device in a communal family space.
- An accompanying adult (18 years +) must be present at all times.
- Attendees should be dressed appropriately.
- The meeting ID is to remain confidential and not to be shared to anyone that it was not designated to.
- Recording, photos or screenshots of the Zoom meeting are **not** allowed by participants.
- The Zoom meeting may be recorded by the hosting teacher and stored online with the school's Acceptable Use Policy.
- The Zoom meeting will be locked by the teacher who will have rights to allowing pupils enter the meeting via the waiting room.
- For participants, some Zoom facilities will be disabled by the host teacher. This includes but is not limited to the screen record function, chat and screen share.
- Lastly, inappropriate online behaviour will not be tolerated and the teacher retains the right to terminate a pupil's participation.

General

- In circumstances where teaching cannot be conducted on the school premises, teachers will use the online platform Seesaw to assist with distance teaching and learning.
- The school has signed up to the terms of service of Seesaw.
- The school has enabled the most up to date security and privacy features which Seesaw provides.
- Staff members will adhere to school guidelines on the use of Seesaw for live engagement.
- Parents/ guardians must sign a consent form for their children to engage with teachers and SNAs using Seesaw/Zoom.
- Parents/guardians must agree to monitor their child's participation in any such lessons and to be in the room with the child for any one-to-one meetings or classes.

- Children will be expected to follow school guidelines on online behaviour.
- In school, every effort is made to ensure child safety, with supervision at all times when using internet. Safe-Surfing settings, on school devices, will be used in order to minimise the risk of exposure to inappropriate materials.
- Pupils and teachers will be provided with training in the area of internet safety and digital citizenship. During Covid 19 closures, parents/guardians will be directed to www.webwise.ie to access guidelines re: online safety.
- Uploading and downloading of non-approved software is not permitted.
- Anti-Virus software will be used and updated as necessary.
- The use of personal memory sticks in school requires a teacher's permission.
- Students and staff will observe good online etiquette at all times. They will not undertake any actions that may be considered disrespectful to members of the school community, or bring the school into disrepute.
- School staff has access to all files used on school computers.
- School devices may record details of what pupils have viewed on the internet. These records may be reviewed by school staff.
- In the case of devices loaned to families during Covid 19 school closures, an agreement will be signed by parents/guardians about its safekeeping and safeguarding of child for whom its use is intended.

World Wide Web

- Pupils or staff will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Pupils will use the internet for educational purposes only.
- Pupils and staff will be educated regarding copyright issues relating to online materials.
- Pupils will never disclose or publicise their own or others personal information
- Pupils or staff will be aware that any internet usage may be monitored for unusual activity, security and/or network management reasons.
- Pupils will never arrange a face-to-face meeting with someone that they have "met" on the internet.

Email

- Pupils may only use parent/guardian approved email accounts under the supervision of or with permission from a teacher.
- Pupils or staff will not intentionally send or receive any material that is illegal, obscene or defamatory or that is intended to harm or intimidate another person.
- Pupils must have permission to send and open email attachments.

School Social Media

- Pupils, in consultation with their teachers, will be given the opportunity to publish their work through Seesaw, the school website and the school Facebook page.
- The publication of student work will be co-ordinated by their teacher.
- Digital photographs, audio or video clips of individual students will not be published on the school sites. Instead these will focus on group activities. Individual pupils will not be identified by name.
- Pupil's home address and contact details will be omitted from school publications
- Pupils will continue to own the copyright on any work published.
- During the school year, parents/guardians are requested not to share any photos of children other than their own, on their social media, without permission.

This includes photos which they may take themselves at school events, or photos shared by the school.

Legislation

There is no specific legislation governing internet safety at school level. Complicating this issue is the fact that the internet functions in a global context whereas the law operates in a localised one. There are, however; a number of key pieces of legislation that have relevance to internet safety. Copies of each of these acts can be found online. All teachers, students and parents should familiarise themselves with these acts. They are briefly described as follows:

- The Data Protection Act 2018: This legislation confers rights on individuals in relation to the privacy of their personal data as well as responsibilities on those persons holding and processing such data. Eight principles of data protection must be adhered to by all organisations and businesses.
- Anti-Bullying Guidelines for Primary Schools 2013.
- Communications Regulation Act (Amendment) 2007: Any individual who sends false offensive indecent, menacing or obscene messages on a phone for purpose of causing annoyance, inconvenience or needless anxiety is committing an offence.
- The Child Trafficking and Pornography Act 1998: This act legislates against anyone who

knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

- 1993 Interception Act: (The Interception of Postal Packets and Telecommunications Messages Regulation Act 1993). This act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.
- Video Recordings Act 1989: The 1989 Video Recordings Act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer.

Sanctions

- If any of the above conditions/rules are broken, it will result in a temporary or permanent ban on internet and/or computer use.
- Additional disciplinary action may be taken in line with existing approved school practice.

Distance Learning/Remote Learning Policy

Guidelines for good online communication in St. Mary's National School Castlefinn

- **Under no circumstances can pictures or recordings be taken of video calls.**
- Staff, families and students are expected to behave in an appropriate, safe, respectful and kind manner online.
- **It is the duty of parents/guardians to supervise children while they are working online and to ensure any content which they are submitting to their teacher is appropriate.**
- Staff members can communicate with pupils and their families via email, Zoom or Seesaw.
- Any electronic forms of communication will be for educational purposes and to allow for communication with families.
- Students and staff will communicate using tools which have been approved by the school and of which parents have been notified (Seesaw & Zoom).
- Parental permission will be acquired before setting up a profile for a pupil on a communication forum.
- **For video calls, parental permission is implied, as the link to a video call will be communicated via the parent/guardian's email address. Essentially, by virtue of the pupil logging on to the call, permission is assumed.**
- For security reasons, passwords will be provided to families, where applicable.
- St. Mary's National School Castlefinn cannot accept responsibility for the security of online platforms, in the event that they are hacked.
- Communication using a mobile phone will not be frequent, but in the rare exception where it is necessary, staff members will ensure that their caller ID is private.

Guidelines for staff members using online communication methods

- Under no circumstances can pictures or recordings be taken of video calls.
- Staff members will communicate with pupils and families during the hours of 9:00am – 3:00pm where possible.
- Staff members will have high expectations regarding pupil behaviour, with any communication which takes place online.
- Staff members will seek to become familiar with apps before using them with pupils.
- Staff will check that consent has been given, before setting up a pupil profile for an online app.
- Staff members will report any concerns regarding online behaviour or interactions to school management.
- Staff are encouraged to generate a new meeting ID and password for each Video meeting being held.
- Staff members will notify parents/guardians of the date, time and password for a video call via email.
- Staff members will only admit participants to video conferences, if they recognise the email address/username as being connected to a pupil.

Rules for pupils using online communication methods

For submitting learning:

- Submit work and pictures that are appropriate - have an adult take a look at your work before you send it.
- Use kind and friendly words.

For video calls:

- Pictures or recordings of the video call are not allowed.
- Remember our school rules - they are still in place, even online.
- Set up your device in a quiet space, with no distractions in the background.
- Join the video with your microphone muted.
- Raise your hand before speaking, just like you would do in class.
- If you have the chance to talk, speak in your normal voice, using kind and friendly words.
- Show respect by listening to others while they are speaking.
- Ensure that you are dressed appropriately for the video call.
- Be on time - set a reminder if it helps.
- Enjoy! Don't forget to wave hello to everyone when you join!

Guidelines for parents and guardians

For submitting learning:

- It is the responsibility of parents and guardians to ensure that pupils are supervised while they work online.
- Check over the work which pupils send to their teacher, ensuring it is appropriate.
- Continue to revise online safety measures with pupils.

For video calls:

- Under no circumstances can pictures or recordings be taken of video calls.
- Ensure that the school has the correct email address for inviting you to join apps and meetings.
- The main purpose of a video call is to maintain a social connection between the school staff and pupils at this difficult time. Encourage pupils to listen and enjoy the experience.
- Be aware that when participating in group video calls, you can be seen and heard unless you are muted or have disabled your camera.
- You will automatically enter a waiting room when the code for a call has been entered. Please note that school staff will only accept users into video call if you can be identified by the display name on your zoom account.
- Please ensure that your child is on time for a scheduled video, or they may be locked out. Please request to join the video call approximately five minutes before the scheduled start time. This will give school staff time to verify your email address.
- Make sure to familiarise your child with the software in advance. For video in particular, show them how to mute/unmute and turn the camera on/off.
- Participants in the call should be dressed appropriately.
- An appropriate background/room should be chosen for the video call.

It is important to note that any breach of the above guidelines will result in a discontinuation of this method of communication. A breach may also result in a person being immediately removed from a meeting or in a meeting being immediately terminated. In this case, the child's parent will receive a report on the incident.

Roles and Responsibilities

It is the overall responsibility of the entire school staff, with the support of parents and pupils, to ensure that these guidelines are implemented within the school environment.

Policy Review

St. Mary's Acceptable Use Policy will be reviewed regularly to ensure it is compliant with current legislation and school practice. The review will be led by the leadership team in consultation with school management, staff, pupils and parents/guardians.

Ratification and Communication

The Board of Management of St. Mary's National School Castlefinn ratified this revised policy at its meeting on _____. A copy will be made available on the school website.

Signed: _____ Date: _____
Chairperson

Signed: _____ Date: _____
Principal

Acceptable Usage Policy

Appendix 1: Permission Form

Dear Parent/Guardian,

Please review the school's Internet Acceptable Use Policy on www.stmarysnscastlefinn.com and sign and return this permission form to the school secretary.

Name of Student: _____ **Class:** _____

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety and the school cannot be held responsible if students access unsuitable websites.

I accept the above paragraph
(Please tick as appropriate)

I do not accept the above paragraph

In relation to the school website and Facebook page, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the site/forum. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

I accept the above paragraph
(Please tick as appropriate)

I do not accept the above paragraph

Signature: _____ Date: _____

As the parent or legal guardian of the above student, I have read the Remote Learning Policy and grant permission for my son or daughter or the child in my care to access online platforms deemed suitable by the class teacher i.e. Seesaw. I understand that access to these online platforms is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access inappropriate content in their own home.

I accept the above paragraph
(Please tick as appropriate)

I do not accept the above paragraph

Signature: _____ Date: _____

Acceptable Usage Policy

Appendix 2: Reproduction Permission Letter

I _____ (Child's name) and _____ (Parent/Guardian's name) give permission to _____ (Person(s) requesting permission) to reproduce work belonging to _____ from the school website.

Parent/Guardian Signature

Date