Acceptable Usage Policy

St Joseph's Secondary School
Spanish Point,
Miltown Malbay,
Co. Clare
V95 NW01

www.stjosephsspanishpoint.com

Mission Statement

St. Joseph's is a Catholic school, based on Gospel Values and in the Mercy tradition under the trusteeship of CEIST.
It is characterised by the following:

***Reverence and Respect,** ***Care and Compassion,**
***Responsibility,** ***Tolerance and Inclusion**
***Justice,** ***Hospitality**

Our mission is to:

- Develop and promote the personal, academic and spiritual potential of each student in a caring and disciplined environment.
- Foster a sense of self-esteem, honesty and respect among all members of the school community.
- Assist students in developing appropriate life skills and social awareness.
- Offer direction and leadership in the educational field in the local community.

CEIST Charter

The core values of CEIST are intended to support and nourish the lives of the people at the heart of our school: students, staff and parents. Its key principles focus on:

- Promoting spiritual and human development
- Achieving quality in teaching and learning
- Showing respect for every person
- Creating community
- Being just and responsible

Acceptable Use Policy

The aim of this Policy is to ensure that students will benefit from learning opportunities offered by the school's ICT & Internet resources in a safe and effective manner.

Internet use and access is considered a school resource and privilege. Therefore, if the school's Acceptable Use Policy is not adhered to, this privilege will be withdrawn and appropriate sanctions – as outlined in the Expected Use Policy – will be imposed.

Digital Technologies Covered

St. Joseph's Secondary School, Spanish Point, will provide students with access to a variety of Digital Technologies and resources including: Internet access, desktop computers, digital imaging equipment, laptop or Chrome book/tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, online discussion forums and email.

This document is intended to cover all Digital Technologies and resources used in the school, not just those specifically mentioned. As new technologies emerge, St. Joseph's Secondary School, Spanish Point, will consider their educational merits and may provide access to them if appropriate.

St. Joseph's Secondary School, Spanish Point Digital Technology Network

St. Joseph's Secondary School, Spanish Point, computer network is intended for educational purposes, therefore:

- All activity over the network may be monitored and retained.
- Access to online content via the network is restricted (web filter).
- Internet content is restricted in accordance with St. Joseph's Secondary School, Spanish Point's policies and Department of Education and Skills policies.
- Students are expected to respect that the web filter is a safety precaution, and therefore should not try to circumvent it when browsing the Web. If a site is blocked and a student believes it should not be, the student can request his/her teacher to submit the site for review. VPNs or other methods of avoiding those terms and conditions will be deemed as in conflict with the school AUP and appropriate sanctions will be imposed.
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline – these rules are found in the St. Joseph's Secondary School, Spanish Point's *Code of Positive Behaviour and Practice.*
- Misuse of school resources may result in disciplinary action as per the Code of Behaviour.
- St. Joseph's Secondary School, Spanish Point will make a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.
- Students are expected to alert his/her teacher immediately of any safety or security concerns.

St. Joseph's Secondary School, Spanish Point email and online collaboration

St. Joseph's Secondary School, Spanish Point provides students with email accounts for the purpose of ***school-related communication.*** Availability and use is restricted based on school policies. Email accounts should be used with care. Email usage will be monitored and archived.

St. Joseph's Secondary School, Spanish Point, recognises that online collaboration is essential to education and may provide students with access to a variety of online tools that allow communication, sharing, and messaging among students. Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.

Use of videoconferencing - Reasonable Use

Our school utilises video conferencing during periods of school closure. Distance learning is a way of learning remotely without being in regular face-to-face contact with a teacher in

the classroom. There are many benefits to teaching and learning in this way, and students and teachers have the tools and expertise to use teleconferencing to sustain learning.

Our school provides a video conferencing option through Google Meet and Zoom Pro for our students and staff. It is expected that students and staff will use the platform in a professional and ethical manner for the purpose of teaching, learning and assessment.

The use of videoconferencing requires students and teachers to observe the following rules in order to ensure that both staff and students benefit from this way of teaching and learning.

Students and Staff should never:

- Post, stream or transmit any content, including live video, that violates this Policy in such a way that is offensive to students / staff.
- Do anything illegal, facilitate any illegal activity, or promote violence.
- Do anything that threatens, exploits or otherwise harms children or fellow students.
- Engage in any activity that is harmful, obscene, or indecent. This includes offensive gestures, displays of nudity, violence, pornography, sexually explicit material, or criminal activity.
- Engage in any activity that is fraudulent, false, or misleading.
- Engage in any activity that is defamatory, harassing, threatening or abusive.
- Store or transmit any data or material that is fraudulent, unlawful, harassing, libellous, threatening, obscene, indecent or otherwise inappropriate.
- Send unauthorised messages or irrelevant material.
- Misrepresent a user's identity or affiliation with any entity or organisation, or impersonate any other person.
- Harvest, collect, or gather user data without consent.
- Violate or infringe any intellectual property or proprietary rights of others, including copyrights.
- Violate the privacy of others or distribute confidential or personal information of others.
- Engage in any activity that is harmful or disruptive to the operation of on-line classes. This includes transmitting viruses, malware or other malicious or destructive code or using tools that mask IP address location or to otherwise circumventing restrictions on use due to regulations or account closures.
- Knowingly performing any act that will interfere with the normal operation of computers, peripherals or networks. Knowingly destroying the integrity of computer-based information.

- Deliberately wasting computer resources.

If school authorities are made aware of any abuse or infringement on these rules, the school will investigate the issue and take immediate, appropriate action where warranted in line with the school's Code of Positive Behaviour and Practice.

School-owned mobile devices

St. Joseph's Secondary School, Spanish Point may provide students with laptops, tablets, digital recorders, or other devices to promote learning both inside and outside of the school. Students should abide by the same expected use policies, when using school devices off the school network, as on the school network.

Students are expected to treat these devices with respect. They should report any loss, damage, or malfunction to a teacher / staff member immediately. Students may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices will be monitored.

Student-owned mobile devices

This policy is in conjunction with our Yondr Policy. St Joseph's is a phone-free school where students place their mobile phones in a Yondr Pouch. In the event students opt not to use the Yondr Pouch, a signed declaration form is completed stating they will leave their phones at home at all times. Students may be allowed to use personally-owned devices (e.g. laptops, tablets-computers, digital-cameras, and smart-phones) for educational purposes with their teacher's permission. Exemptions are given for students who need to use a mobile phone for medical reasons. The unauthorised capture of images, video or audio is in direct breach of the School's AUP.

Network Security

Students are expected to take reasonable safeguards against the transmission of security threats over the school network.

- This includes not opening or distributing infected files or programmes and not opening files or programmes of unknown or untrusted origin.
- Students should use common sense if they think a website does not appear to be appropriate. If in doubt, students should bring their concern to the attention of their teacher. They should reflect carefully before opening any website that does not appear to be appropriate.
- If a student believes a computer or mobile device they are using might be infected with a virus, they should alert their teacher to their concern.
- Students should not attempt to remove the virus themselves or download any programmes to help remove the virus.

- Students should not download or attempt to download or run programmes with an execute extension (i.e. any programme ending with the suffix *.exe*). However, with their teacher's permission, students may be permitted to download other file types, such as images or videos.
- For the security of the St. Joseph's Secondary School, Spanish Point, images and videos should only be downloaded from reputable sites and only for educational purposes.

Netiquette

Netiquette is defined as appropriate rules of etiquette (social behaviour) that apply when communicating over computer networks and especially when communicating online. Therefore:

- Students should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognise that among the valuable content online, there is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the Internet.
- Students should not post anything inappropriate online, a simple rule would be, anything that a student would not want their parents, teachers, peers, colleagues or future employers to see. Once something is posted online, it is there for anyone to see and often be shared and spread in ways that was never intended.

Plagiarism

- Students should not plagiarise content (copy or use as your own without citing the original creator), including words or images, from the Internet.
- Students should not take credit for work they did not create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.
- The school may check for plagiarism using online tools as are available for such purposes.

Personal Safety

- If students views a message, comment, image, etc., online that makes them concerned for their or their peers' personal safety, they must bring their concern immediately to the attention of their teacher, parent or guardian
- Students should never share personal information about themselves or others, including phone numbers, addresses, PPS numbers and birth-dates, etc., over the Internet

- Students should never agree to meet someone they met online

Cyber-bullying

Harassing, flaming, denigrating, impersonating, outing, tricking, excluding and cyber-stalking are all examples of cyber-bullying.

- Such bullying will not be tolerated in St. Joseph's Secondary School, Spanish Point.
- Students should not send emails or post comments or images with the intent of scaring, hurting, or intimidating someone else.
- Students should not engage in any online activities intended to harm (physically or emotionally) another person, such activities will result in severe disciplinary action and loss of privileges.
- Students should be aware that in some cases, cyber-bullying is a crime.
- Students should also be aware that their online activities are monitored and retained.
- The school will support students, teachers and parents in dealing with cyber-bullying.

Violations of this Expected Use Policy

Violations of this policy in St. Joseph's Secondary School, Spanish Point, may have disciplinary repercussions, including:

- Written Warnings
- Suspension of network and computer privileges
- Notification to parents in most cases
- Detention
- Suspension from school and/or school-related activities
- Expulsion
- Legal action and/or prosecution

Acceptable Use Policy

I will:

- Use school technologies for school-related activities and research
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline
- Treat school resources with care and alert teachers if there is any problem with their operation
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies
- Alert a teacher if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts, etc.) online
- Use school technologies at appropriate times, in approved places, for educational pursuits only
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement
- Recognise that use of school technologies is a privilege and treat it as such
- Be cautious to protect the safety of myself and others
- Help to protect the security of school resources

I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others
- Search inappropriate images or content
- Engage in cyber-bullying, harassment, or disrespectful conduct toward others
- Try to find ways to circumvent the school's safety measures and filtering tools
- Use school technologies to send spam or chain mail
- Plagiarise content (copy, use as their own, without citing the original creator) found online
- Post personally-identifying information, about myself or others
- Agree to meet someone offline that has been met online
- Use unacceptable or inappropriate language online
- Use school technologies for illegal activities or to pursue information on such activities
- Attempt to access unsuitable sites, inappropriate servers, accounts, or content

These are not intended to be exhaustive lists. Students should use their own good judgment when using school technologies.

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____ _____

(Student Printed Name) (Student Signature)

I have read and discussed this Acceptable Use Policy with my child:

_____ _____

(Parent / Guardian Printed Name) (Parent / Guardian Signature)

_____

(Date)

Review and Amendments to Policy

This Policy will be subject to regular monitoring and review. This Policy will be reviewed by school management and may be revoked, replaced or amended at any time and stakeholders will be informed accordingly.

Policy Ratified: 15/09/2022

Policy Review: 2027

Signed: _____ Signed: _____

(Chairperson of Board of Management) (Principal)

Date: 15/09/2022 Date: 15/09/2022