Diocese of Orlando / Office of Catholic Schools
Student Technology Responsible Use Policy
2023-2024

1.0 Introduction

St. Joseph Catholic School recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to technologies for student and staff use.

This Technology Responsible Use Policy outlines the guidelines and behaviors that students are required to follow when using school technologies or personally owned devices on and off school campus.

- The St. Joseph Catholic School network is intended for educational purposes.
- All activity over the network or when using school technologies will be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources or personal devices while connected to the school network or outside network can result in disciplinary action.
- St. Joseph Catholic School makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the school network or other technologies are required to alert Administrator, Technology staff or teacher immediately of any concerns for safety or security.

2.0 **Definitions**

2.1 Authorized Users:

- **Student:** any child 18 years or younger enrolled in St. Joseph Catholic School
- **Faculty/Staff:** any person who is employed by St. Joseph Catholic School, whether part-time or full-time, who provides instruction or supports the school operations.

2.2 **School Network**: communications systems connecting two or more computers and their peripheral devices to exchange information and share resources, it includes wired and wireless

2.3 **Internet:** includes both external and internal access of communications and data storage equipment, either owned or reserved for use by St. Joseph Catholic School.

2.4 **Technologies Covered:** St. Joseph Catholic School may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. Also, St. Joseph Catholic School may allow students to bring their personal devices which will also be covered by this policy.
As new technologies emerge, St. Joseph Catholic School will attempt to provide access to them. The policies outlined in this document are intended to cover ***all*** **available technologies**, not just those specifically listed.

3.0 Usage Policies

All technologies provided by the school are intended for education purposes. All students are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; do not try to get around technological protection measures; use good common sense; and ask if you do not know. In the event that the inappropriate behavior happens outside of the school, it is disrupting instrucition, and it is brought to the principal's attention, St. Joseph Catholic School will investigate and may have disciplinary repercussions at the discretion of the school according to the Code of Conduct.

3.1 **Web Access**

St. Joseph Catholic School provides its students with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with Diocesan Social Communication Policy, CIPA (Children's Internet Protection Act) regulations and school policies. Web browsing is monitored and web activity records may be retained indefinitely.

Students are expected to respect that the web filter is a safety precaution, and 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 should follow school protocol to alert Technology staff or submit the site for review.

3.2 **Email**

St. Joseph Catholic School may provide students with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If students are provided with email accounts, they should be used with care. Students should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the school policy or the teacher.

Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived. Student's password(s) are not to be shared with anyone.

3.3 **Social / Web 2.0 / Collaborative Content**

Recognizing the benefits collaboration brings to education, St. Joseph Catholic School may provide students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging will be monitored by teachers and the sites will be protected from outside viewers. Students should be careful not to share personally-identifying information online.

The use of personal social media sites for enjoyment is prohibited on campus during instructional hours. Students must refrain from taking and posting pictures and videos of themselves, other students or teachers at school during instructional hours. Also, creating fake accounts using the school's name, logo or any other symbol that identifies as a school sanction account will be asked to be deleted and the student will face disciplinary action and loss of privileges.

3.4 **Livestreaming**

For distance education, St. Joseph Catholic School will implement a video conferencing platform that will allow teachers to livestream instruction to students at home. It is important to know that classes will be streamed in a secured platform with encryption of data in transit, password protection, will not be recorded, and only students assigned to the class will have access to it. The camera will be focused on the teacher and the content presented to the class.

Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct as if they were present in the classroom. In addition, they must not try to record or take screenshots of the livestream. If they need further assistance, they should schedule time to talk to the teacher. It is required that students at home wear their school uniforms and that a quiet space is provided to avoid disruptions or distractions to the teacher and other students.

3.5 **Mobile Devices Policy**

St. Joseph Catholic School may provide students with mobile computers or other devices to promote learning outside of the classroom. Students should abide by the same responsible use policies when using school devices off the school network as on the school network.

Students are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to the student's care. Students should report any loss, damage, or malfunction to the Technology staff immediately. Students may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

3.6 **Personally-Owned Devices Policy**

St. Joseph Catholic School may allow students to bring personally owned devices to use in the classroom after it has been approved by the Technology staff. Students should keep personally-owned devices (including laptops, tablets, e-readers, smart phones, cell phones, and smart watches) turned off and put away during school hours unless as instructed by a teacher or staff for educational purposes or in the event of an emergency.

Because of security concerns, when personally-owned mobile devices are used on campus requiring the use of data, these devices must only be on the school network, data services must be disabled and permission from the Technology staff is required. For the Technology staff to grant permission, students need to submit the required paperwork with the appropriate information such as MAC address and serial number. In some cases, a separate network may be provided for personally-owned devices.

Students must follow the same code of conduct for use of personally owned devices on St. Joseph Catholic School campus or at other functions, whether on or off property, related to the St. Joseph Catholic School.

3.7 **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 programs and not opening files or programs of unknown or untrusted origin.

If the student believes a computer or mobile device the student is using might be infected with a virus, IT must be alerted immediately. The student must not attempt to remove the virus or download any programs to help remove the virus. Passwords need to be unique to each student and not shared with other students.

3.8 **Downloads**

Students should not download, attempt to download, or run .exe programs or any other executable programs over the school network or onto school resources without express permission from the Technology staff.

Students may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, only for education purposes, and following copyright laws.

3.9 **Netiquette**

Students should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the Internet and follow copyright laws for their use.

Students should also remember not to post anything online that they would not want parents, teachers, or future colleges or employers to see. Once something is online, it is out there—and can sometimes be shared and spread in ways it was never intended.

3.10 Plagiarism

Students should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Students should not take credit for things 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.

4.0 **Personal Safety**

Students should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without permission from a parent or legal guardian. Students should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Students should never agree to meet someone they meet online in real life without parental or legal guardian permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you are at school; parent or legal guardian if you are using the device at home) immediately.

5.0 Cyber Bullying

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Do not be mean. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

6.0 **Sexting**

Any student taking, disseminating, transferring, possessing, or sharing obscene, sexually oriented, lewd, or otherwise illegal images or other content, commonly referred to as “sexting,” which can include, but is not limited to, pictures of themselves, other students or friends without appropriate clothing or in compromising or suggestive positions, will be disciplined according to the Student Code of Conduct, may be required to complete an educational program related to the dangers of this type of behavior, and, in certain circumstances, may be reported to law enforcement. This type of behavior needs to be immediately reported to the parent/guardian, and if it involves other students in the school it should be reported to the teacher or principal.

7.0 Examples of Responsible Use

The student will:

- ✔ Use school technologies for school-related activities.
- ✔ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✔ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✔ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✔ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- ✔ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ✔ Cite sources when using online sites and resources for research.
- ✔ Recognize that use of school technologies is a privilege and treat it as such.
- ✔ Be cautious to protect the safety of others and myself.
- ✔ Help to protect the security of school resources.

This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

8.0 Examples of Irresponsible Use

I, the student will **not**:

- ✔ Use school technologies in a way that could be personally or physically harmful.
- ✔ Attempt to find inappropriate images or content.
- ✔ Engage in cyberbullying, 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.
- ✔ Plagiarize content I find online.
- ✔ Post personally identifying information, about others or myself.
- ✔ Agree to meet someone I meet online in real life.
- ✔ Send or distribute obscene, lewd or sexually explicit images.
- ✔ Use language online that would be unacceptable in the classroom.
- ✔ Use school technologies for illegal activities or to pursue information on such activities.
- ✔ Attempt to hack or access sites, servers, or content that is not intended for my use.

This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

9.0 Internet Safety Plan

- ✔ St. Joseph Catholic School implements an effective internet filtering and reporting solution Sophos, that monitors internet activity, and uses current technologies to detect inappropriate usage and block and/or filter visual depictions that are obscene, pornographic or in any way harmful to minors as defined in CIPA
- ✔ The internet filtering solution is in place to control access by minors to inappropriate matter on the Internet and the World Wide Web and restrict access to materials that may be harmful to minors
- ✔ Policies and procedures are in place that covers category blocking, automated weekly reports on internet activity, and identification of emerging threats
- ✔ School network is secure with Sophos to prevent from unauthorized access, including "hacking" and other unlawful activities by minors online
- ✔ Faculty provides internet safety instruction integrated in their curriculum or as part of a technology class that covers appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber bullying
- ✔ Technology Responsible Use Policy and Internet Safety Plan will be published in the parent/student handbook and St. Joseph Catholic School will hold an informational meeting to address the policy.

10.0 Limitation of Liability

- ✔ St. Joseph Catholic School will not be responsible for damage or harm to any personal devices, files, data, or hardware brought to the school by students.
- ✔ While St. Joseph Catholic School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
- ✔ St. Joseph Catholic School will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

11.0 Violations of this Responsible Use Policy

Violations of this policy may have disciplinary repercussions at the discretion of St. Joseph Catholic School, according to the Code of Conduct, and including but not limited to:

- Suspension of network, technology, or computer privileges

- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

12.0 References

- ✔ Children's Internet Protection Act – http://www.fcc.gov/cgb/consumerfacts/cipa.html , http://ifea.net/cipa.html
- ✔ Children's Online Privacy Protection Act - http://www.ftc.gov/ogc/coppa1.htm
- ✔ Protecting Children in the 21st Century - http://www.ntia.doc.gov/legacy/advisory/onlinesafety/BroadbandData_PublicLaw110-385.pdf
- ✔ Consortium for School Networking – http://www.cosn.org

I understand that inappropriate and irresponsible use and conduct while using the device and/or other technology resources and/or school network shall result in appropriate disciplinary action. I agree to be a responsible digital citizen and user and will conduct myself appropriately while online. I have read and understood this Responsible Use Policy and agree to abide by it:

_____

(Student Printed Name)

_____ _____

(Student Signature) (Date)

As a parent/guardian, I will or have discussed Responsible Use Policy, user guide, and all other policies with my child and will support the school in guiding my child in using the device at home as an educational tool. I understand that I am responsible for monitoring and guiding my child's activity while he/she is not at school.

_____

(Parent/Legal Guardian Printed Name)

_____ _____

(Parent/Legal Guardian Signature) (Date)