



# ST. JOHN PAUL II CATHOLIC SCHOOL

## Student/Staff Technology Responsible Use Policy

### Purpose

St. John Paul II Catholic School recognizes that access to technology in schools 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 technology for student and staff use. The purpose of this Responsible Use Policy is to:

- Emphasize that access to technology is provided for educational purposes that support the mission, vision, core beliefs and goals of St. John Paul II Catholic School
- Enhance the development of 21st Century Skills alongside the Indiana Academic Content Standards
- Encourage innovation, communication, creativity, collaboration and problem-solving skills by providing access to current and relevant information
- Prepare students for college or career

### Definition of Technology

- Internet, shared network resources and external file storage devices
- Desktop, mobile computers (Chromebooks), tablets (iPads) and other handheld devices
  - This includes school owned and personal devices.
- Videoconferencing, televisions, projection systems and telephones
- Online collaboration, message boards, and email
- Copiers, printers and other equipment
- Additional technologies, as developed

### CIPA

St. John Paul II Catholic School is in compliance with the Children's Internet Protection Act (CIPA) and has installed technology protection measures for all computers in the school corporation. A technology protection measure is in place that blocks or filters Internet access. This filter protects against access by adults and minors to visual depictions that are obscene, pornography, or — with respect to use of computers with Internet access by minors — harmful to minors. The content filter does monitor the online activities of minors and may be reviewed. While CIPA specifically pertains to internet usage by minors, St. John Paul II expects that faculty and staff will follow these same guidelines for responsible use. Additionally, there is no expectation of privacy for users who access our network or use technology (school-owned or personal) on school property.

The Responsible Use Policy (RUP) applies to:

- School-owned technology on the St. John Paul II Catholic School Internet/network, on non-school networks and offline
- Privately owned technology that is connected to the St. John Paul II Catholic School internet/network and on privately owned networks while on school property

## **Responsible Use**

Users must abide by all school rules as outlined in the Student Handbook and this Responsible Use Policy. This policy outlines the guidelines and behaviors that all users are expected to follow when using technology. It is the responsibility of both St. John Paul II Catholic School and parents to help prepare students to be members of a digital society or digital citizens. Digital citizenship is defined as the norms of behavior with regard to technology use.

A digital citizen is one who:

1. Understands human, cultural, and societal issues related to technology and practice legal and ethical behavior.
2. Advocates and practice safe, legal, and responsible use of information and technology.
3. Exhibits a positive attitude toward using technology that supports collaboration, learning, and productivity.
4. Demonstrates personal responsibility for lifelong learning.
5. Exhibits leadership for digital citizenship.

## **Prohibited Use**

Unacceptable uses of school electronic resources include, but are not limited to:

1. Accessing or Communicating Inappropriate Materials—Users may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages. St. John Paul II reserves the right to make determinations about what is considered inappropriate.
2. Prohibited Activities—Users may not use the school district's computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. St. John Paul II Catholic School and its employees and agents assume no responsibility for illegal activities of students while using school computers or school-issued electronic resources. Additionally, it is not permissible to use the St. John Paul II Catholic School Internet/Network for personal business or commercial purposes.
3. Violating Copyrights or Software Licenses—Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.
4. Plagiarism—Users may not represent as their own work any materials obtained on the Internet (such as term papers, articles, music, etc). When using other sources, credit must be given to the copyright holder. Users should not take credit for things they didn't 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.

5. Cyberbullying – Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, and cyberstalking are all examples of cyberbullying. Do not send emails or post comments with the intent of scaring, hurting, or intimidating others. 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. Misuse of Passwords/Unauthorized Access –Users may not share passwords; use any user account/password that is not assigned to them; or attempt to circumvent network security systems.

7. Malicious Use/Vandalism–Users may not engage in any malicious use, disruption or harm to the school district’s computers, electronic devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

8. Avoiding School Filters–Users may not attempt to use any software, utilities or other means to access Internet sites or content blocked by the school filters.

9. Unauthorized Access to Blogs/Social Networking Sites, Etc. – Users may not access blogs, social networking sites, etc. prohibited by school administration or the St. John Paul II Catholic School Technology Department (Five-Star Technology Solutions). Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.

10. Degrade System Resources - Users shall not use the network in such a way that would degrade the performance system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects, as determined by the supervising instructor or school administrator.

11. Unauthorized Equipment - Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the district network without permission from the school administration or St. John Paul II Catholic School Technology Department (Five-Star Technology Solutions).

## **Privacy**

All computers, telephone systems, voice mail systems, electronic mail, and electronic communication systems are the district’s property. The district retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with district’s computer, telephone, electronic mail, and voice mail. Furthermore, all electronic communications and information may be archived, deleted, monitored, and reviewed at any time. Students and staff should have no expectation that any information contained on such systems is confidential or private.

## **Safety and Security**

1. All users are given accounts upon entry into St. John Paul II Catholic School. Any user account given is intended for the sole use of that user only. Each user is responsible for the security of the system. Passwords should not be shared. If a user shared a password with another, that user will be held accountable.
2. Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as websites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.
3. Staff may post student pictures on district/ school/classroom “public” websites as long as the student’s name or other identifying information is not included. Students’ grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.
4. Many devices have the capability to record audio and video. Students may not use devices to record, transmit, or post photos or videos of a person or persons on campus unless directed by a supervising person as part of an assignment or classwork. The use of cameras in any type of electronic device is strictly prohibited in locker rooms and restrooms (as well as before/after school).
5. St. John Paul II Catholic School staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).
6. Students may be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

## **Damage/Liability**

Users may be responsible for compensating the school district for any losses, costs or damages incurred for violations of Board policies/procedures and school rules, including the cost of investigating such violations. The school district assumes no responsibility for any unauthorized charges or costs incurred by users while using school district computers, devices, or the school network.

The school is not responsible for any personal device brought on school property that is damaged, lost or stolen.

## **GRADE 6-8 TAKE HOME DEVICE INFORMATION: Breakage/Lost/Stolen Device**

If a student’s device is broken, lost, or stolen and parents do not opt to purchase insurance on the device, the parents are assuming financial responsibility for the cost of repairs/replacement. All breaks must be reported immediately to the student’s teacher. Only St. John Paul II may repair and replace devices; in other words, parents may not use an outside party of their choosing to repair devices and parents are not permitted to purchase a replacement device on their own (only St. John Paul II may purchase new/replacement devices). Parents will be billed for all costs.

If students lose their charger, they must tell their teacher immediately and will need to purchase a new charger through the school. Students may not purchase a charger on their own. The fee to replace a chromebook charger is \$50.

If students lose their device, they should report it immediately to their teacher. It is important that students report any missing devices ASAP so that St. John Paul II Catholic School can assist in locating the device. If students lose their device and it cannot be located, they will be responsible for the full cost of replacement (approximately \$300.00). If a student's device is broken, lost, or stolen; this must be reported immediately.

- Insurance for grade 8 is optional (but recommended). Even if you have not purchased this insurance in the past, you can still purchase it for this year. The insurance may be purchased through the Worth Ave. Group (this is the same insurance company we have used in the past). The cost is \$29 per device with a \$0 deductible. Parents interested in purchasing insurance may do so by visiting <https://www.worthavegroup.com/gpo/stjohnpaulschool> . There is no other approved option for purchasing insurance. **The deadline to purchase coverage is August 14.**
- Grades 6 and 7 devices include insurance so no additional insurance needs to be purchased.
- In order to file a claim for a stolen device, a police report is required.

## Terms of Use

St. John Paul II Catholic School reserves the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, including suspension or expulsion from school, for violations of this policy. Additionally, all handbook regulations apply to the use of the St. John Paul II Catholic School's network, Internet, and electronic resources.

## Disclaimer

St. John Paul II Catholic School, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, St. John Paul II Catholic School is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.
2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.
3. Unauthorized financial obligations resulting from the use of St. John Paul II Catholic School's electronic resources.

## **ACCEPTANCE AND COMPLIANCE OF RUP**

### Examples of Responsible Use:

I will:

1. Use technologies for school-related activities.
2. Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline. Be courteous and respectful.

3. Not post any information that I would not want students, parents, teachers, or future colleges or employers to see (once something is online, it is available to the world).
4. Treat school resources carefully, and alert staff if there is any problem with their operation.
5. Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
6. Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
7. Use technologies at appropriate times and in approved places, for educational pursuits.
8. Cite sources when using online sites and resources for research.
9. Be prepared for class by making sure my device is charged.
10. I will follow all expectations for responsible use outlined by my teacher and/or St. John Paul II Catholic School.
11. Be cautious to protect the safety of others and myself.
12. Help to protect the security of school resources.
13. I will use technology for school-related purposes only (assignments and/or class work).

### **Examples of Unacceptable Use:**

I will not:

1. Use school technologies in a way that could be personally or physically harmful.
2. Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Responsible Use Policy.
3. Create a personal mobile “hotspot” or utilize a “proxy site” for the purpose of circumventing network safety measures and filtering tools.
4. Create, distribute or deploy multi-user servers or gaming software on or within the St. John Paul II Catholic School’s network.
5. Engage in cyberbullying, harassment, or disrespectful conduct toward others.
6. Try to find ways to circumvent the school’s safety measures and filtering tools; intent to circumvent safety measures and filtering tools is a violation of this Responsible Use Policy.
7. Use technologies to send spam or chain mail.
8. Plagiarize content I find online.

9. Post or otherwise disclose personally identifying information, about others or myself.
10. Agree to meet someone I meet online in real life.
11. Use language online that would be unacceptable in the classroom.
12. Use technologies for illegal activities or to pursue information on such activities.
13. Attempt to hack or access sites, servers, or content that isn't intended for my use.

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

Violation of this policy may result in loss of access as well as other disciplinary action.