Digital Citizenship & Acceptable Use Policy

At St. Joseph Catholic STEM School, technology is a powerful tool for learning, creativity, communication, collaboration, and service. As a Catholic STEM school, we seek to form students who use technology with wisdom, integrity, self-control, and respect for the God-given dignity of every person.

We call our students to be **Digital Disciples**, young people who use technology in ways that honor God, respect others, seek truth, protect human dignity, and contribute to the common good.

Access to school technology is provided to support learning and the mission of St. Joseph Catholic STEM School. Students are expected to use these resources responsibly, safely, ethically, and in accordance with this policy.

This policy applies to school-owned devices, school networks, school-provided accounts, school-approved applications and services, and personal devices when brought onto school property or used in connection with school activities.

1. The Five Habits of a Digital Disciple

- **PROTECT**: Safeguard personal information, passwords, and accounts. Immediately notify a trusted adult if unsafe, threatening, or inappropriate content is encountered.
- **RESPECT**: Recognize that every person is created in the image and likeness of God. Communicate with Christian charity and never use technology to bully, humiliate, demean, or exclude others.
- **THINK**: Pause and evaluate whether content, searches, or AI prompts are truthful, appropriate, safe, and helpful before clicking or sharing.
- **CREATE**: Use digital tools to learn, solve problems, and produce good works rather than as a source of distraction.
- **BE HONEST**: Maintain academic integrity, complete original work, give proper credit to sources, and use artificial intelligence responsibly.

2. Personal Electronic Devices (Device-Free School Day) To protect instructional time, minimize distractions, and cultivate personal relationships, the school maintains a personal device-free environment during school hours.

- **Scope**: Includes (but not limited to) cell phones, smartwatches, earbuds/AirPods, headphones, personal tablets, gaming devices, and recording equipment.
- **Storage**: Personal devices brought to school must remain turned off and stored in the student's locker or designated area throughout the day.
- **Wearables**: Smartwatches and communication wearables are permitted only if kept in a locked "school mode" that prevents communication, games, and internet access. An exception from the school office will be needed to do this.

- **Communication & Exceptions**: Parents needing to contact students during the school day must call the main office. Exceptions are granted by administration for documented medical or educational accommodation plans.
- **Liability**: Students are responsible for their personal property; the school is not liable for lost, stolen, or damaged items.

3. School Technology, AI, & Academic Integrity

- **School Property & Accounts**: School-issued email addresses, devices, networks, and cloud storage are educational property. Students must use assigned credentials, keep passwords private, treat equipment carefully, and report damage immediately.
- **Our Catholic Approach to AI:** St. Joseph School aims to develop students to become wise users of internet-enabled tools. Pope Leo XIV has called families and schools to an "educational alliance for the digital age." At St. Joseph, that means teaching students not only *how* to use Artificial Intelligence, but how to discern *when, why, and whether* it should be used. We embrace the idea that technology should strengthen human learning and relationships; not replace thinking, creativity, effort, friendship, or our search for the good, the true and the beautiful.
- **Academic Honesty**: Submitting AI-generated work as original effort, using AI to cheat, or entering confidential student data into unapproved AI tools is strictly prohibited.

4. Digital Communication, Media & Human Dignity

- **Consent & Privacy**: Students may not photograph, record audio/video, or capture screenshots of others without explicit teacher authorization and permission.
- **Protection of Image**: Creating, requesting, storing, or sharing inappropriate or private images is prohibited.
- **Synthetic Media & Impersonation**: Using AI, editing software, or fake accounts to fabricate misleading, humiliating, or altered images, voices, or representations of community members is strictly forbidden.
- **Off-Campus Conduct**: Digital behavior outside of school hours that impacts student safety, school operations, or community dignity remains subject to school disciplinary authority.

5. Safety, Monitoring, & Response Protocols

- **Network Monitoring**: The school utilizes **Securly Classroom** (teacher management), **Securly Filter** (content blocking), and **Securly Aware** (flagging safety risks like cyberbullying or self-harm). Students have no expectation of privacy on school-provided accounts, networks, or devices.

- **Stop. Close. Tell. Protocol**: When accidentally encountering inappropriate, violent, or troubling content, students should follow three steps:

    1. **STOP**: Discontinue viewing, clicking, or sharing immediately.
    2. **CLOSE**: Close the application, screen, or message.
    3. **TELL**: Inform a teacher, parent, or trusted adult right away.
- **Restorative Reporting**: Students who accidentally encounter inappropriate material and report it promptly will be supported restoratively, distinguishing them from those who intentionally search for or share harmful content.

Content filtering software is not 100% accurate. Sometimes it will not flag sites that are actually inappropriate. It is crucial that students report inappropriate content immediately.

6. Unacceptable Uses & Cybersecurity

Students may not use school technology to:

- Access or share violent, adult, sexually explicit, hateful, or discriminatory content.
- Attempt to bypass filters using VPNs, proxies, personal hotspots, or alternate DNS services.
- Gain unauthorized administrative access, alter system settings, or introduce malware.
- Engage in cyberbullying, harassment, threats, or unauthorized commercial activities/gambling.
- Install unauthorized software or access non-educational games and streaming services.

7. Policy Consequences

Violation Type	Progressive Administrative Action
Personal Device Violations	**1st Offense**: Device confiscated to office until end of day; optional $10 fine supporting local food shelf. **2nd Offense**: Device confiscated; parent retrieval required or 2-day office check-in. **3rd & Repeated**: Extended daily device check-in, parent conference, or loss of device privileges on campus.
Technology & Network Misuse	Actions vary by severity: reteaching, restriction of digital privileges, parent conferences, financial restitution for intentional equipment damage, suspension, or law enforcement referral for major safety breaches.

8. Family Partnership & Research Parents serve as the primary educators in building healthy digital habits. Families are encouraged to model healthy usage, establish tech-free zones (meals, prayer, bedtime), keep devices out of bedrooms overnight, and maintain open dialogue regarding online pressure and social media.

Key Research Resources for Families

- **Ledger of Harms** (ledger.humanetech.com): Highlights the psychological impact of engagement-driven platforms on adolescents.
- **Institute for Family Studies** (ifstudies.org): Examines correlations between smartphone overuse, social media, and adolescent mental health.
- **Canadian Medical Association Journal** (pmc.ncbi.nlm.nih.gov/articles/PMC7012622/): Links heavy screen exposure to sleep deprivation, distress, and reduced academic focus.
- **Dr. Michael Ungar** (psychologytoday.com): Outlines the value of structured cell-free zones paired with active offline social substitutes.

Digital Disciple Policy Agreement

Student Agreement I have read and agree to follow the Digital Citizenship & Acceptable Use Policy. I commit to practicing the Five Habits of a Digital Disciple—to Protect, Respect, Think, Create, and Be Honest. I understand that violations may result in restricted technology access or disciplinary action.

Student Name: _____ Grade: _____ Date: _____

Student Signature: _____

Parent/Guardian Agreement I have reviewed this policy with my child. I support the school's standards regarding personal devices, educational technology, monitoring, artificial intelligence, and digital stewardship.

Parent/Guardian Name: _____ Date: _____

Parent/Guardian Signature: _____