

# IMMACULATE HEART CENTRAL SCHOOL SYSTEM TECHNOLOGY ACCEPTABLE USE POLICY

Updated November 2025

Technology is a valuable and real-world educational tool. Immaculate Heart Central School System is committed to teaching students, faculty, administrators, staff, and the broader school community to work and learn effectively and responsibly with technology. This policy defines expectations for responsible, ethical, and secure use of technology in support of our Catholic mission and educational goals.

# Student Acceptable Use Policy

Immaculate Heart Central Schools provide computing devices, networks, and cloud-based systems (Google Workspace for Education, Chromebooks, and other approved tools) for educational purposes. Access to these systems is a privilege, not a right, and carries responsibilities. Students must use technology in a way that upholds the school's mission, respects others, and follows all local, state, and federal laws.

## Appropriate and Ethical Use

Students are expected to use technology for educational purposes only. Any use that disrupts learning, harasses others, or violates school values is prohibited. Students may not access, create, or distribute inappropriate, obscene, or discriminatory materials. They may not use technology to cheat, plagiarize, or misrepresent their work.

## Artificial Intelligence Tools

Students may not use artificial intelligence (AI) tools such as ChatGPT, Copilot, Google Gemini, or similar systems to complete academic assignments or assessments unless explicitly permitted and supervised by a teacher. AI use must never replace a student's own learning or integrity of work. Teachers may utilize AI or digital literacy tools for instructional purposes to help students understand responsible and ethical technology use. The school reserves the right to use AI-detection tools to verify academic integrity.

## Device and Network Security

Students are responsible for the care and security of any school-issued device. Devices should not be modified or used to bypass filters or monitoring. Attempts to access restricted areas, disable security settings, or use unauthorized software will result in disciplinary action.

## Personal Device and Network Access

Students are not permitted to connect personal devices, including but not limited to cell phones, laptops, tablets, Chromebooks, smartwatches, or gaming devices to the school's Wi-Fi or wired network. The school network is reserved exclusively for school-owned and managed devices. Any attempt to connect an unauthorized device, share network credentials, or create hotspots on campus is a violation of this policy and may result in disciplinary action and loss of privileges.

## Internet Safety and Privacy

The school uses content filters and monitoring systems to comply with the Children's Internet Protection Act (CIPA). Students must never attempt to bypass these protections. Personal information, including full names, home addresses, phone numbers, or photos, must not be shared online without permission. The school reserves the right to monitor all activity conducted on its networks or devices.

## Social Media

Students must demonstrate good judgement and respect when engaging online. Posting photos, videos, or messages involving the school, staff, or other students without authorization is prohibited. Cyberbullying or any online harassment that affects the school environment may result in disciplinary action and possible referral to law enforcement.

## Cell Phone and Smart Devices

For cell phone usage, please check pages 33 and 34 in the handbook. Recording, photographing, or sharing classroom activities without permission is strictly prohibited.

## Consequences of Misuse

Misuse of technology may result in suspension, revocation of technological privileges, disciplinary action, and potential liability for damages. The school reserves the right to investigate suspected misuse and confiscate devices when necessary.

## Technology Maintenance, Inspection, and Monitoring

All school-issued devices and accounts remain the property of Immaculate Heart Central School. The school reserves the right to inspect, reimage, or remotely manage any device to maintain security, update software, or ensure compliance with this policy. Students and staff should have no expectation of privacy in data stored on or transmitted through school systems.

## Student and Parent/Guardian Internet Access Agreement

We have read and discusses the Immaculate Heart Central School Technology Acceptable Use Policy. We understand and agree to the expectations outlined. I give permission for my child to use school technology and internet resources under supervision. I understand that all activity may be monitored.

Student Name: \_\_\_\_\_

Grade: \_\_\_\_\_

Student Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Parent/Guardian Name: \_\_\_\_\_

Parent/Guardian Signature: \_\_\_\_\_

## Faculty, Staff, and Administration Acceptable Use Policy

Faculty, staff, and administrators are entrusted with technology resources to support teaching, learning, and administrative responsibilities. The use of technology must reflect professionalism, confidentiality, and the moral teachings of the Catholic faith.

### Professional and Ethical Conduct

All staff must use school systems solely for authorized purposes. Personal use should be limited and never interfere professional duties. Staff are expected to model appropriate and respectful technology use for students.

### Data Privacy and Security

Staff must protect student and employee information in compliance with FERPA, COPPA, and CIPA regulations. Sensitive data must not be stored on personal devices or shared outside approved systems. Strong passwords and two-factor authentication must be used when able.

### Social Media and Public Representation

Staff should maintain appropriate boundaries with students and colleagues online. “Friending” or direct messaging students through personal accounts is discouraged unless it serves an official educational purpose. All online communication should reflect the values and professionalism expected of Catholic educators.

### Security and Incident Reporting

Any suspected data breach, phishing attempt, or unauthorized access must be reported immediately to IT. Staff should never share credentials or attempt to bypass filters or security protocols. Technology use may be monitored to ensure compliance with school policy.

### Acknowledgment and Compliance

All staff members must sign this agreement upon hiring. Violation of these guidelines may result in disciplinary action up to and including revocation of access privileges or termination, as appropriate.

## Faculty, Staff, and Administration Internet Access Agreement

I have read and understand the Immaculate Heart Central School Technology Acceptable Use Policy. I agree to use school technology systems in accordance with these expectations and understand that violation of this policy may result in disciplinary action.

Employee Name: \_\_\_\_\_

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_\_