

ACCEPTABLE USE AGREEMENT 2026-2027



Our Lady of Mount Carmel

Catholic Elementary School

Philosophy & Purpose

Technology at OLMC serves the school's Catholic mission—forming students in love, truth, beauty, and mercy—and supports rigorous learning, collaboration, creativity, and research. We teach digital citizenship, ethics, privacy, and balance (including the value of unplugging and face-to-face relationships). Technology is a gift to be used wisely: to build community, communicate with charity, and advance learning in partnership with families. All use must be educational, lawful, safe, respectful, and aligned to school policy.

1. Scope, Ownership & Monitoring

All OLMC devices, networks, accounts, and technology program assets are school property and remain under the control, custody, and supervision of the school. Use is a privilege—not a right—and may be suspended or revoked. The school may monitor, log, filter, and review all activity (including email, files, and internet traffic) without notice. Students have no expectation of privacy. Web filtering is used but cannot block all content.

2. Acceptable Use & User Responsibilities

Use technology for curriculum-aligned educational purposes and under teacher/administrator direction. Respect self/others; protect personal information; safeguard passwords; cite sources; and comply with all instructions, laws, licenses, and school policies. Report unsafe/inappropriate content or security problems immediately.

3. Prohibited Uses (examples, not exhaustive)

- Harassing, threatening, deceiving, intimidating, offending, or embarrassing any person; cyberbullying.
- Posting/using defamatory, false, obscene, profane, lewd, violent, abusive, or sexually explicit content or language.
- Using/creating/posting photos, images, video, likeness, live streams, or school logos without required permission from the individual(s) and the principal.
- Creating unauthorized websites, social media accounts, or online content that impersonates the school or members of the school community.
- Accessing another person's files/accounts; using someone else's credentials; forging/intercepting communications.
- Attempting to bypass or disable filters/security/anti-virus software including hotspots or other circumvention tools; altering configurations.
- Installing, moving, deleting, reconfiguring, or modifying software/hardware without authorization.
- Accessing unauthorized social media/gaming/entertainment sites, websites or online material inconsistent with the school's educational mission.
- Plagiarizing or violating copyright/license terms; submitting others' work as one's own.
- Using technology for commercial, fraudulent, or illegal activity; breaching confidentiality obligations.
- Any action that harms the goodwill/reputation of the school or creates substantial disruption.

4. Privacy, Safety & Security

- Students must not share full names, addresses, phone numbers, or personal details without teacher permission.
- Never meet contacts from the internet without parent permission; report dangerous/inappropriate content immediately.
- System Security: Report security issues to administration; do not share this information with other students; violations may result in loss of privileges and disciplinary/legal action.
- Digital Security: Users should enable the highest available level of account security, including two-factor or multi-factor authentication whenever available.

- Storage Devices: Use of external devices or removable drives is discouraged; limited use may be permitted only with attention to security.
- Email: The school's email system is for education-related purposes; it is not private. Unauthorized access is prohibited. Users are responsible for the content of messages they create; no forging/intercepting communications.
- Privacy Laws: All users must comply with applicable privacy laws, including FERPA and COPPA, and maintain the confidentiality of student and school records.

5. Educational Applications, Communication & Social Media

- The school utilizes approved third-party educational applications and cloud-based services. (e.g., school-issued email, FACTS SIS, Google Classroom, and other approved apps).
- Use only school-sanctioned educational applications and communications to ensure the privacy and security of our students and school. Personal email may not be used for school business.
- Teachers/staff should not distribute personal phone numbers; occasional calls may occur but numbers should not be published.
- No friending/following current students on personal social media; teachers should maintain professional accounts if needed.
- Administrative approval is required for any school-related social media account; create with a school-issued email; maintain at least two adult moderators.
- Do not post student audio/photo/video that reveals a student's face or voice without prior parental authorization. Use first name and last initial on school-sanctioned accounts; do not tag/link to student personal accounts.
- Personal and professional posts must be respectful and must not disclose confidential information about students, staff, or families.

6. Audio/Video Recording

Unauthorized recording (audio or video) on school grounds, during class, meetings, phone calls with school personnel, or school events is prohibited without prior consent from all participants and approval from the classroom teacher and/or administration. Educational recordings by teachers may occur for approved instructional purposes with the required permissions.

7. Artificial Intelligence (AI)

Students are prohibited from using AI tools (e.g., ChatGPT, Google Gemini, Microsoft Copilot) to complete assignments, quizzes, or exams unless a teacher or administrator explicitly authorizes and supervises their use. Any AI tools approved for classroom use must comply with applicable privacy laws and Archdiocesan AI requirements. Submitting AI-generated content as original work violates academic integrity and is subject to disciplinary action.

8. Personal devices, Games & Non-Educational Use

- The use of cell phones, smart watches, wearable devices, and other personal technology is governed by school policy and may only be used when authorized.
- Consumer smart speakers and always-listening devices (such as Amazon Echo or Google Nest) may not be connected to the school network or used in classrooms.
- Viewing or playing electronic games during school hours is prohibited unless part of a teacher-assigned instructional activity.
- Networked or violent/adult-content games are not allowed.

9. Liability & Enforcement

- OLMC and/or the Archdiocese of Philadelphia are not responsible for data loss, service interruptions, or damages arising from technology use.
- Monitoring and filtering software may be used to block inappropriate content.

- Violations may result in loss of privileges, disciplinary action (including for conduct off-campus that causes substantial disruption), reimbursement for damages/costs, and/or legal action.