Technology Acceptable Use Policy 2025/2026

Lourdes Academy permits access to computer, telecommunications, and Internet resources to further the educational quality of the material available through these resources. It is the purpose of this policy to ensure acceptable practices by students in regard to computers, telecommunications, or use of any technology. Our system is committed to teach its students, staff, and school community to work and to learn effectively to ensure responsible use of technology. The policy outlined below applies to all technology device use including but not limited to internet usage.

Uses mentioned in this document apply to inside the school use and may, in certain instances, apply to personal technology use and/or uses outside of school. Where personal outside use of technology threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students or teachers to participate fully in school or co-curricular activities, these activities may be viewed as a violation of the Acceptable Use Policy and may be subject to disciplinary measures.

The types of electronic and digital communications referenced in this AUP include, but are not limited to social networking sites, cell phones, digital cameras, text messaging, email, VOIP, chat rooms, and instant messaging.

The System's goal is to prepare its members for life in a global digital community. To this end, the System will:

- Integrate technology with curriculum to enhance teaching and learning
- Encourage critical thinking, communication, collaboration, and problem-solving skills
- Facilitate evaluation and synthesis of information
- Require ethical practices and provide education for internet safety and digital citizenship along with proper care/etiquette of any devices.
- Provide a variety of technology-based tools and related technology skills

Best Practices and Procedures for Students

1. Students will not be granted access to their device or other technology until both they and a parent/guardian have signed this AUP and any other relevant documents that may be required. There are no exceptions to this.
2. Access to the school's programs, email, and similar electronic communications systems is a privilege and certain responsibilities accompany that privilege. Users are expected to demonstrate the same level of ethical and professional manners as is required in face-to-face or written communication.
3. Understanding your actions in the digital space leaves lasting records and impressions. Think carefully and act responsibly before posting or doing anything online. Ensure your actions are in alignment with the Lourdes Law and make good choices. This includes Social Media Site, any Public Forums, as well as any collaboration with other students in an online environment.
4. Never use Technology to perform any actions that might be considered unethical, illegal, or cause harm to someone else. This also applies to any actions that might circumvent rules or tools in place to ensure a safe learning environment.

5. Use of cell phones during the school day is a privilege and subject to the same rules and guidelines as any device issued by Lourdes. The principal or administration will determine when devices may be used during the day.
6. Students will not use technology to hack or access any other persons account/files/etc
7. Students agree to not post pictures, videos or other files that include images of other students without their express permission. Many things once posted to the digital space can never truly be removed.

Privacy

1. There is not a right to privacy when using the school's technology resources. School personnel may review files and communications to maintain system integrity and ensure that users are using the system responsibly and appropriately. Authorized personnel will have the right to review any and all material saved, transmitted, accessed, or momentarily in use by the user. Users should not expect any privacy when using the network or devices at Lourdes.
2. All activity over the school network or using system technologies may be monitored and retained.
3. Any information contained or placed on the school's devices, Online Storage, or any other space owned by Lourdes is property of Lourdes.

Notes: Administrators and the IT Department are required and morally obligated to investigate any specious activities occurring on school computers and report suspicious activity to administration. Lourdes uses and maintains various tools to assist in protecting the safety of its staff, students and campus

Copyright and Plagiarism

1. Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the internet. Users 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.
2. Users are to respect the right of intellectual property of other people and to respect all copyright laws. If a user is unsure whether copyright law is being respected, they need to raise the question with the staff member with this expertise.
3. Students should discuss with their teachers what constitutes acceptable use of AI in doing their coursework (IE: using ChatGPT, Gemini, other AI based tools/sites to generate answers or work that is then submitted). When in doubt, exercise caution and seek approval first.

Cyber-bullying

1. Cyber-bullying is considered an act of harassment and will not be tolerated. Harassing, dissing, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyber-bullying. Do not send emails, texts, post

comments, or use other forms of digital communication with the intent of scaring, hurting, or intimidating someone else.

2. Users should never communicate false information or engage in personal, prejudicial, or discriminatory attacks.
3. Engaging in cyberbullying 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 in which case, police will be involved. Remember that your activities may be monitored and retained.

Safety

1. Online stalkers and identity thieves are a real threat. Never share personal information, including but not limited to, social security numbers, phone numbers, addresses, exact birth dates, financial information, and pictures.
2. Users should never agree to meet someone they met online in real life without parent permission.
3. Always verify information you find online. While there are many reputable sources, there are also just as many illegitimate sites and sources with false information. You are responsible for verifying the accuracy of any information you find.
4. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety or if you feel violated, harassed, uncomfortable, or accosted through the school's technology resources, bring it to the attention of an adult (teacher or staff if at school, parent if you are at home.). Lourdes is committed to the safety of students and staff.

CIPA (Children's Internet Protection Act) Compliance

It is the policy of Lourdes Academy to make a good faith effort to (a) prevent users (students, staff, minors, adults) access over its computer network to, or transmission of, inappropriate material via internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; (d) comply with the Children's Internet Protection Act [Pub. L No. 106-554 and 47 US 254(h)]. Internet usage will be monitored and implemented per Board policy, State and Federal statutes. The following categories are subject to regulation via the above policies:

- Access to inappropriate material
- Supervision and monitoring
- Inappropriate network usage
- Key terms as defined in the Children's Internet Protection Act

Security

1. Users should keep their passwords secure and never share passwords with others. If someone tampers with your accounts without you knowing about it, you could be held accountable.

2. Users of the system network or other technologies are expected to alert technology staff immediately of any concerns for safety or security or any problem with its operation.
3. Users 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.
4. If you believe a computer or mobile device you are using might be infected with a virus, you need to alert the technology staff immediately. Do not attempt to remove the virus yourself or download any programs to help remove the virus.
5. Users are not to try to find a way to circumvent the school's safety measures and filtering tools.
6. Users are not to attempt to hack or access sites, servers, or content that is not intended for their use.

Damage and Vandalism

1. Students should never tamper with or vandalize the property of the school or other users including equipment, cabling, and other infrastructure; any security system that protects the school's computer resources; and data. Users are not to tamper with, remove components from, or otherwise deliberately with the operation of computers, networks, printers, or other associated peripherals.
2. Vandalism is further defined, but not limited to, deleting, examining, copying, or modifying files, data, email, or voice mail belonging to other users, and/or attempts of the same; attempts to breach security codes and/or passwords; and/or destruction, abuse or codification of computer hardware and/or software including changes to preferences, and/or attempts of the same.
3. The Lourdes Academy Catholic School System will not be held liable for any damage, loss or theft of any personal property brought to school, including technology devices.
4. This agreement applies to stand-alone units as well as units connected to the network or the internet.

Consequences

Users need to recognize that the use of school technology is a privilege and not a right and should treat it as such. Students are expected to follow the same rules for good behavior and respectful conduct online as offline.

1. Any attempt to violate the provisions of this agreement will result in the suspension/revocation of the user's privileges, regardless of the success or failure of the attempt. In addition, disciplinary action, and/or appropriate legal action may be taken. The decision of the administrator is final. The administration reserves the right to seek restitution for damage necessitating repair of replacement software, equipment, network, and systems.
2. Lourdes Academy maintains the right to confiscate any cell phone, or other personal electronic found on school premises or used at school. If a device is

taken away, it will be returned at the end of the day, or possibly referred to parents or law enforcement if malicious activity is suspected.

3. The system reserves the right to enforce guidelines within the Student Handbook for misconduct, whether inside or outside school, that is detrimental to the reputation of the school.
4. Violations of this policy may have disciplinary repercussions for students, including suspension of network, technology, or computer privileges; payment of any damages caused; detention, suspension or expulsion from school or school-related activities; and legal action and/or prosecution.