Holy Name provides technologies and computer/electronic services access for the enhancement of education. The intent of these guidelines is to allow the greatest use of our computing resources consistent with the goals and objectives of our schools and the guiding principles of Catholic/Christian Education.

1. Access to the Internet must be for the purpose of education or research, and be consistent with the educational and religious objectives of the school.
    - Computers and the Internet will only be used for legal activities. Illegal activities include but are not limited to the following:
    - Failure to follow copyright laws.
    - Failure to cite sources.
    - Illegal copies of music, games, etc. in students possession or loaded onto technologies
    - Accessing files, emails, accounts of other students/staff
    - Making unauthorized copies of software.
    - Operating technologies including but not limited to computers, tablets, laptops and media in a manner that makes the equipment unusable. Examples include:
2. Willful destruction of technologies including media. Willful destruction may include:
    - Forcing anything into the ports and slots on the devices
    - Jerking, dropping or slamming the device and cover, if available.
    - Carrying a laptop or chromebook by its cover
    - Putting chromebook on the floor, edge of desk or unstable surface
    - Throwing the device
    - Eating or drinking in vicinity of device
    - Removing the device from the classroom without permission, putting the device in student's locker or bookbag, taking the device from the building
    - Intentional overloading the computer's resources,
    - Creating, propagating, and/or willfully using computer viruses
3. Technologies may not be altered without permission of the school's technology director. Examples include:
    - Loading/downloading programs/software and apps
    - Downloading files as a means for copying or storing any software, music, shareware, or freeware.
    - Changing the parameters of the computer, including background and screensaver.
    - Attempting to access to the Internet without the approved filtering program/service or firewall required by NCLB regulations and prevailing laws.
4. Due to privacy issues, use of personal Email accounts or social media sites at school without teacher permission is not allowed. A school email address *may* be provided for web based projects. This address is available for the duration of the school year and used only for educational purposes.
5. Communication in and out of the building must adhere to strict guidelines. The following are prohibited:
    - Sharing personal information as stated in Federal Law CIPA requirements.
    - Submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, or sexually-oriented, threatening, racially offensive, harassing, or illegal material.
    - Sending information using an account created for another student.
    - Advertising or promoting any illegal activities or content inconsistent with school policies
    - Using abusive or racial language
    - Threatening other students or school staff online
    - Posting pictures taken at school of other students or staff on social media (SnapChat or other site) without their parent's consent or staff consent.
6. Network users may not attempt to access other files. "Hacking" or otherwise trying to gain access to another person's or organization's computer system or password is prohibited.
7. If a student should accidentally enter a site with inappropriate material, it is the student's responsibility to immediately close out of programs, files, or sites that do not meet the lesson objectives. Any other student or supervising adult observing, share in this responsibility.

8. All digital products are the property of the school. Content may be reviewed at any time. The content may be used in web pages and for publicity purposes. ***Web pages designed and posted by the school staff and students will never have the student's full name. The school Facebook site may include pictures of classes and activities. Pictures will not be labeled or tagged with student's full name.***
9. Students should have no expectation of privacy in their use of school computers, the Internet, or e-mail. Administrators and faculty may review files and messages to maintain system integrity and insure that users are acting responsibly.
10. In the event social networking sites are made available to students for instructional and educational purposes, parents will be notified prior to usage and given instructions for joining the social networking site if they choose.

School Staff Responsibilities *(Excerpt from Adult Policy):*

- Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the CUES Schools.
- Staff must instruct the students in school policies and train them in Internet Safety.
- Staff should make reasonable efforts to become familiar with the Internet and the student Acceptable Use Policy so that effective monitoring, instruction, and assistance may be achieved.
- All use of the Internet must be in support of educational and research objectives consistent with the mission and objectives of Holy Name School.

The use of the Internet is a privilege, not a right, and inappropriate use, whether in school or outside of school, will result in a cancellation of those privileges. Illegal use of the technologies may result in suspension or expulsion. Employees and students have no expectation of privacy in their use of school computers, the Internet, or e-mail.

_____ _____/_____/_____
Student **Date**

_____ _____/_____/_____
Student **Date**

_____ _____/_____/_____
Student **Date**

_____ _____/_____/_____
Student **Date**

Parent Agreement (to be signed by parents of all student users under the age of eighteen)
As parent or guardian of above student(s), I have read the Acceptable Use Policy. I understand that this access is designed for educational purposes. CUES Schools have taken reasonable steps to control access to the Internet, but cannot guarantee that all controversial information will be inaccessible to student users. I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission for my child to use network resources, including the Internet. ***If I allow my child to bring their personal device to school, I recognize that my child holds full responsibility for the safety of the device. The school will not be held liable for any damage or theft.*** If the device is found in use by any staff member during school hours without express permission, it will be given to the principal. **The parent/guardian will be responsible for picking up the device from the principal.**

_____ _____/_____/_____

Parent /Guardian **Date**

_____ _____

Date Checked **Signature of Teacher/Administrator**

http://e-ratecentral.com/CIPA/cipa_policy_primer.pdf Policy is based on Federal Laws listed on the CIPA (Children's Internet Protection Act) site.