Student
Acceptable Use Policy
St. Mary School, Elyria
Diocese of Cleveland

St. Mary School, Elyria (the "School") makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the school, its students and its employees. The Acceptable Use Policy ("Policy") is intended to minimize the likelihood of such harm by educating the School's students and setting standards that will serve to protect the school. We firmly believe that digital resources, information and interaction available on the computer, network or Internet far outweigh any disadvantages.

Definition of school technology system: The school systems and networks (collectively, "System") are any configuration of hardware and/or software whether used on or off school property. The System includes, but is not limited to, the following:

- telephones, cellular telephones, and voicemail technologies;
- email accounts;
- servers;
- desktop and laptop computer hardware and peripherals;
- software including operating system software and application software including without limitation video conferencing software;
- digitized information including stored text, data files, email, digital images, and video and audio files;
- internally or externally accessed databases, applications, or tools (Internet- or District-server based);
- school provided Internet access;
- school filtered public Wi-Fi;
- school provided Chromebooks;
- school provided personal digital assistants ("PDAs"), tablets, IPADs and similar devices;
- school issued access to third party websites (i.e., Google apps, Zoom, Flipgrid, Dojo, etc.) ; and
- new technologies as they become available.

Acceptable Use: Students are responsible for appropriate behavior on the System just as they are in a classroom or on a school playground. Communications on the System are often public in nature. General school rules for behavior and communications apply. It is expected that users will comply with school standards and the specific rules set forth below as interpreted from this policy, whether on or off of school property. A student is personally responsible for his/her actions in accessing and utilizing the school's computer resources in accordance with Student Code of Conduct and may be subject to discipline for misuse of the System.

Access to communication system: Access to the school's electronic communications system, including the Internet, shall be made available to students for educational and instructional purposes. Each school computer/device and Wi-Fi (available for students who bring in their own personal telecommunication devices) has filtering software that block access to visual deceptions that are obscene, pornographic, inappropriate for students, or harmful to minors as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA.

Access to the School's computer/network/Internet is a privilege, not a right, and may be revoked at any time.

Scope of Use: The System is intended for use for educational and instructional purposes only. Incidental, personal use shall be allowed only so long as such use is appropriate for a school setting, non-disruptive to the school's operations and mission, and not in excess or to the exclusion of the student's studies or school responsibilities.

Inappropriate Use: Inappropriate use includes, but is not limited to, those uses that are specifically named as violations in this document; that violate the rules of network etiquette; or that hamper the integrity or security of the System or any components that are connected to it.

Transmission on the System, including through email (personal or school accounts), social media, web pages, blogs and/or forums, of any material in violation of any federal or state law or this Policy is prohibited. This includes, but is not limited to:

- cyber bullying;
- threatening, pornographic, harassing, defamatory or obscene material;
- copyrighted material, plagiarized material or materials protected by trade;
- the use of hardware and/or software which disrupts or interferes with the safety and welfare of the school community (even if such uses take place after school hours or off school property).

Vandalism or Mischief: Tampering with or theft of components from the System may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a school computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the school will fully comply with the authorities to provide any information necessary for legal action.

Modification of Computer: Modifying or changing computer/device settings and/or internal or external configurations without appropriate permission is prohibited and may result in discipline and/or the revocation of access to the System.

Student Access: System access is provided to all students unless parents or guardian request in writing to the school principal that access is denied. When student is in a classroom setting on school property, student Internet accesswill be under the direction and guidance of a school staff member. Students must adhere to the following guidelines when using the System on or off of school property:

1. Respect and protect the privacy of others.
    a. Use only assigned accounts.
    b. Decline to view, use, or copy passwords, data, or networks to which they are not authorized.
    c. Avoid distribution of private information about others or themselves.
    d. Decline to record any individual, educational instruction or any portion of communications without prior written consent of teacher or school administration.
2. Respect and protect the integrity, availability, and security of all electronic resources.
    a. Observe all network security practices as posted.
    b. Report security risks or violations to a school administrator, teacher or network administrator.
    c. Refrain from destroying or damaging data, networks, or other resources that do not belong to them without clear permission of the owner.
    d. Conserve, protect, and share these resources with other students and Internet users as appropriate.
    e. Get appropriate pre-approval before accessing the network with personal devices.
    f. Abstain from overriding the Internet content filtering system.
3. Respect and protect the intellectual property of others.
    a. Refrain from copyright infringement (making illegal copies of educational lessons, music, games, or movies).
    b. Avoid plagiarism.
4. Respect and practice the principles of parish and school community.
    a. Communicate only in ways that are kind and respectful.
    b. Report threatening or discomforting materials (cyber bullying) to a school administrator, teacher or network administrator.
    c. Refuse to access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).

d. Avoid accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
e. Abstain from using the resources to further other acts that are criminal or violate the school's code of conduct.
f. Avoid sending spam, chain letters, or other mass unsolicited mailings.
g. Refrain from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.
h. Avoid posting or disseminating any harassing, demeaning, threatening or immoral comment or visual injurious to the reputation of the school, the parish, the Church or an individual, whether the action occurs on school property or off grounds.

5. Abide by the Student Code of Conduct in the use of the System at all times.

School Email and Communication tools: Email and other digital tools such as, but not limited to, blogs and wikis are tools used to communicate. The use of these communication tools should be limited to instructional, school related activities; or administrative needs. All communications within these tools should adhere to this Policy.

The Use of Video Conferencing: Staff and students may from time to time use video conferencing software for educational purposes, including without limitation Zoom and Google Hangouts.. . Video conferencing is a way that students can communicate with teachers, other students, speakers, othersfrom their school, local community, and/or other parts of the country and the world, in real time. All students agree to the following related to use of video conferencing software whether or not on school property during use:

a) Videoconference sessions may be videotaped by school personnel or by a participating school involved in the exchange in order to share the experience.
b) Students' voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session.
c) Students are only permitted to transmit audio/video images using the System when all of the following conditions are met (i) it is under teacher's direction, (ii) it is for educational purposes, (iii) it is sent only to other classmates or school staff members, and (iv) it is sent during classroom hours.
d) Students shall not record any portion of a videoconferening session without prior written approval from teacher or school administration.
e) Students shall not save, share, post or distribute in any way any part of a videoconferencing session or any photos or audio recording from a videoconferencing session without prior written approval from teacher or school administration.
f) All sessions must be set up soley by school personnel and communcicated to students and/or parents privately and not through any public domain.
g) Classroom and school rules apply to all remote learning experiences.

The following guidelines must be adhered to by students using a personally-owned telecommunication device at school or with the System whether on of off school property:

a. All personally-owned telecommunication devices must be registered with the Technology Coordinator prior to use.
b. Internet access is filtered by the School on personal telecommunication devices in the same manner as School owned equipment. If network access is needed, connection to the filtered, wireless network provided by the school is required. Use of any service bypasses the security filter and is considered a violation of the Acceptable Use Policy.
c. These devices are the sole responsibility of the student owner. The school assumes no responsibility for personal telecommunication devices if they are lost, loaned, damaged or stolen and only limited time or resources will be spent trying to locate stolen or lost items.
d. These devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on school property, including school buses.

e. Each student is responsible for his/her own device: set-up, maintenance, charging, and security. Staff members will not store student devices at any time, nor will any staff diagnose, repair, or work on a student's personal telecommunication device.
f. Telecommunication devices are only to be used for educational purposes at the direction of a classroom teacher.
g. School administrators and staff members have the right to prohibit use of devices at certain times or during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) that occur during the school day.
h. An administrator may examine a student's personal telecommunication device and search its contents, in accordance with disciplinary guidelines.

Subject to Monitoring: All School System usage on or off school property shall not be considered confidential or private and is subject to monitoring by designated staff at any time to ensure appropriate use. All electronic files, including email messages, from both school-issued and personal accounts, transmitted through or stored in the System, will be treated no differently than any other electronic file. The School reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Students should treat the computer system like a shared or common file system with the expectation that electronic files sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the School for any purpose. Personal telecommunication devices are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Acceptable Use Policy has been violated.

Students have no expectation of privacy with respect to use of the System whether on or off school property and whether the device s are school or personally owned. Administrators reserve the right to examine, use, and disclose any data found on the System in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions and/or may refer information to law enforcement if a crime is believed to have been committed.

All computers, chromebooks, devices, laptops, Chromebooks, tablets, or the like, used by students to access the System, including both school-owned equipment and personally-owned devices, are subject to search at any time if a violation of this Policy or other school policies is suspected.

Consequences for Violation: Students have the responsibility to use the System in an appropriate manner which complies with all school policies. Violations of these rules or any school policy may result in disciplinary action which may include the loss of a student's privileges to use the school's information technology resources and/or discipline. Consequences of misuse or abuse of these resources will be disciplined depending on the severity of the situation. In addition to school disciplinary action, appropriate legal action may be taken.

Agreement Form: In order to ensure the proper use of technology resources, it is necessary that each student and parent/guardian *annually* sign the attached Student Acceptable Use Policy – User Agreement Form. The signed form must be on file at the School before Internet and other technology access is permitted. Signing the form indicates that the user will abide by the rules governing Internet and other technology access as stated in this Policy.

The school reserves the right to issue additional or more detailed rules for the use of technology resources, and violations of such rules may be a cause for imposition of any of the penalties delineated above. The school reserves the right to seek financial restitution for any damage caused by a student. Upon its discretion, the school reserves the right to request student/parent complete additional forms prior to the distribution of any electronic devices.