St. Jude School Acceptable Use Policy 2018-2019

Diocese of Cleveland

St. Jude 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 is intended to minimize the likelihood of such harm by educating St. Jude School students and setting standards which 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.

All users are expected to use the technology available at St. Jude School in a manner that is consistent with the teachings and mission of the Catholic Church and the school's academic programs. Technology includes but is not limited to: cellular telephones; CD/MP3/DVD players; personal data devices; computers, hardware and peripherals; software including operating system and application software; Internet; digitized information including stored text, data, email, digital images, video and audio files; internally or externally accessed databases, applications, or tools (Internet- or school-server based); school provided Internet access; and new technologies as they become available.

Users are expected to be appropriately responsible for and use technology to which they have access. Actions considered inappropriate are prohibited and will result in revocation of the student's access to the computer/network/Internet.

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 this computer/network/Internet system or any components that are connected to it.

Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to: cyber bullying; threatening, pornographic, harassing, defamatory or obscene material; or other inappropriate use of technology such as e-mail, social networking, web pages, and 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).

Students must:

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.

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.

e. Refrain from accessing the network with personal devices without approval of school administration.

f. Abstain from overriding the Internet content filtering system.

g. Refrain and/or minimize at all times damaging devices and their assigned cases, both at school and at home (applies to Chromebook).
At no time should a student mark, write, place stickers, color or deface in any manner Chromebooks, iPads, laptops and computer lab computers or any other school device. Damage or replacement of said devices and/or cases will be the responsibility of the student/parent.

3. Respect and protect the intellectual property of others.

a. Refrain from copyright infringement (making illegal copies of 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.

Consequences for Violation: Violations of these rules may result in disciplinary action, including the loss of a student's privileges to use the school's information technology resources. Users have the responsibility to use technology resources in an appropriate manner. Consequences of misuse or abuse of these resources will be disciplined depending on the severity of the situation.

Supervision and Monitoring: School and network administrators and their authorized employees periodically will continuously monitor the use of information technology resources to help ensure that users are secure and in conformity with this policy. Students have no expectation of privacy with respect to the use of technology resources. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. The school administration has the right of access to any electronic devices brought onto school property. They may also use this information in disciplinary actions and will furnish evidence of crime to law enforcement should one be committed.

Agreement form: In order to ensure the proper use of technology resources, it is necessary that each user and parent/guardian annually sign the attached Student Acceptable Use Policy – User Agreement Form. The signed form must be on file at St. Jude 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.**

CIPA Compliance & Internet Safety Policy

It is the policy of St. Jude School to: (a) prevent user 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 USC 254(h)].

Definitions:

Key terms are as defined in the Children's Internet Protection Act.

ACCESS TO INAPPROPRIATE MATERIAL

Practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications or access to inappropriate information.

Specifically, as requires by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

INAPPROPRIATE NETWROK USAGE

Practical, steps shall be taken to promote the safety and security of users of the St. Jude School computer network when using electronic mail, chat rooms, instant messaging, social media, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

EDUCATION, SUPERVISION AND MONITORING

It shall be the responsibility of all members of the St. Jude School Staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator or designated representatives.

The Technology Coordinator or designated representatives will provide age-appropriate education and training for students who use St. Jude's Internet facilities. The training provided will be designated to promote St. Jude's commitment to:

A) The standards and acceptable use of Internet services as set forth in the St Jude Internet Safety Policy.

B) Student safety with regards to:

i. Safety on the Internet.

ii. Appropriate behavior while on online, on social networking Web sites, and in chat rooms; and

iii. Cyberbullying awareness and response.

C) Compliance with the E-rate requirements of the Children's Internet Protection Act (CIPA)

Following receipt of this training, the student will knowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

MINOR

The term "minor" means any individual who has not attained the age of 17 years.

TECHNOLOGY PROTECTION MEASURE

The term “technology protection measure” means a specific technology that blocks or filters Internet access to visual depictions that:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code.

2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code.

3. Harmful to minors

HARMFUL TO MINORS

The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT

The term “sexual act” and “sexual contact” having the meanings given such terms in section 2246 of title 18, United States Code.