St. Francis School

ACCEPTABLE USE and INTERNET SAFETY POLICY

St. Francis School

ACCEPTABLE USE and INTERNET SAFETY POLICY
for Employees, Students and Volunteers

Please read the following carefully before signing this document. This is a legally binding document.

Introduction

It is the policy of St. Francis School to: (a) prevent user access over its computer network for, or transmission of, inappropriate material via the 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; and (d) comply with the Children's Internet Protection Act [Pub.L.No. 106-554 and 47 USC 254(h)]. We will adhere to all Diocese of Erie policies and provisions for the protection of children as well as guidelines for Use of Photographic Images of Children and Youth.

Overview

Computers, handheld devices, network, Internet, electronic communications and information systems (collectively "CIS systems") provide vast, diverse and unique resources. Access to the school's electronic communications systems and network is granted to responsible users for educational purposes, and terms of use are outlined in this document. This access includes Internet access, whether wired or wireless, or by any other means.

SECTION ONE: GENERAL COMPUTING POLICY

1) Acceptable Use

In order to ensure smooth system operations, the school administrator has the authority to monitor all accounts. A user must abide by the terms of all software licensing agreements and copyright laws. A user can be monitored at any time. Once a user receives a user ID to be used to access a computer or network and computer systems on that network, he or she is solely responsible for all actions taken while using the user ID. Therefore, the following are prohibited:

a) Applying for a user ID under false pretenses
b) Sharing your user ID with any other person. (If you do share your user ID with another person, you will be solely responsible for the actions of that other person
c) Deletion, examination, copying, or modification of files and/or data belonging to the school or other users without their prior consent
d) Attempts to evade or change resource quotes, posting personal communications without the original author's consent; invading the privacy of others; attempting or gaining unauthorized access to resources or entities; accessing or vandalizing the data of another user; using the network for any unauthorized or illegal activity, including violation of copyright or other contracts; downloading or uploading software
e) Use of facilities and/or services for commercial purposes
f) Any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration
g) Copying programs purchased by you onto the school's computers and/or the network systems, without the express, written consent of the school
h) Copying programs, licensed to the school, for personal use
i) Abusing and disrupting electronic equipment and/or systems

2) Security

It shall be the responsibility of all members of the school staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act (CIPA). To the extent practical, steps shall be taken to promote the safety and security of users of the school's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA prevention of inappropriate network usage includes: (a) unauthorized access, including 'hacking and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors. Appropriate training will be provided for staff and students in the use of technological resources, the Internet and electronic communications.

Subject to administrative approval, technology protection measures may be disabled or minimized, for adult Internet usage only, for bona fide research or other lawful purposes.

As a user of a computer or network, you may be allowed to access other networks and/or computer systems attached to those networks. Therefore, the following are prohibited:

a) Use of systems and/or networks in attempts to gain unauthorized access to remote systems
b) Decryption of system or user passwords
c) Copying, deleting, or moving system files
d) Deleting, examining, copying, or modifying files and/or data belonging to other users
e) Copying of copyrighted materials, such as third party software, without the express written permission of the owner or the proper license
f) The willful introduction of computer "viruses" or other disruptive or destructive programs into the computer and/or network or into external computers and/or networks
g) Vandalism is prohibited, including, but not limited to, any attempt to harm or destroy the data of another user, the network/Internet, or any networks or sites connected to the network/Internet. Attempts to breach security codes and/or passwords will also be considered a form of vandalism.
h) Willful destruction of computer hardware or software or attempts to exceed or modify the parameters of the system are prohibited. Nothing in this policy shall prohibit the school operator from intercepting and stopping E-mail messages which have the capacity to overload the computer resources. Discipline may be imposed for intentional overloading of school computer resources.

SECTION TWO: INTERNET ACCESS

Internet access is available to employees and students of St. Francis School. We believe the Internet offers vast, diverse and unique resources to administrators, teachers, employees, and students. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Administrators, teachers, employees, and students have access to:

- electronic mail communication with people all over the world;
- many University Library Catalogs, the Library of Congress and the Education Resources Information Center, (ERIC);
- a plethora of topics ranging from Japanese culture to music, to politics, to the environment;
- the public domain and shareware of all types

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the school setting. Our school has taken precautions to restrict access to controversial materials. To the extent practical, technological protection measures (or "Internet filters") shall be used to block or filter access to inappropriate information on the Internet, or via other forms of electronic communications. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene, to child pornography, and to any material deemed harmful to minors. However, on a global network it is impossible to control all materials and a user may discover controversial information. We firmly believe that the valuable information and interaction

available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with education goals.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical and legal utilization of the network resources. If a user from our school violates any of these provisions, his or her Internet access will be terminated, and future access could possibly be denied. Disciplinary and/or legal action including, but not limited to, criminal prosecution under appropriate state and federal laws may also be taken. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

INTERNET ACCESS – TERMS AND CONDITIONS

1) Acceptable Use

The purpose of accessing the Internet is to support research and education in and among academic institutions in the United States by providing access to unique resources and the opportunity for collaborative work. Your use must be in support of education and research, and consistent with the educational goals and objectives of our school. Each user is personally responsible to follow these provisions at all times when using the network.

a) Use of other organization's network or computing resources, including "cloud computing" must comply with the rules appropriate for that network.
b) Transmission of any material in violation of local, state and/or federal statutes or regulations is strictly prohibited. This includes, but is not limited to: copyrighted material, material protected by trade secret, threatening material, obscene material, pornographic material and criminal activity.
c) Use for commercial activities or product advertisement (including campaigns for student government/council) is prohibited.
d) Use of the network in any way that would disrupt network use by others is prohibited.
e) NEVER reveal personal information such as your address, phone number, password or social security number. This also applies to others' personal information or that of organizations.
f) Use of the network or computer resources to publicly oppose, degrade, and/or intentionally misrepresent any teachings, beliefs, or practices of the Catholic Church are strictly prohibited.

2) Privileges

The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The school administrator will deem what is inappropriate use and his or her decision is final.

3) Network Etiquette

You are expected to abide by the generally accepted rules of network etiquette (netiquette). These include, but are not limited to, the following:

a) Be polite. Do not send, or encourage others to send, abusive messages.
b) Use appropriate language. Remember that you are a representative of your school and diocese on a non private network. You may be alone on a computer, but what you say can be viewed around the world. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are forbidden.
c) All communications and information accessible via the network should be assumed to be private property.

4) Online Safety and Behavior

St. Francis School, in accordance with amendments to the Children's Internet Protection Act (CIPA) contained in the "Protecting Children in the 21st Century Act" (October, 2008), will include in our technology education program for minors' instruction concerning:

a) Appropriate online behavior;
b) Interacting with other individuals on social networking websites and chat rooms;
c) Cyber bullying awareness and response. "Cyber bullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones.

5) Electronic Mail (E Mail)

Whenever you send electronic mail, your name and user ID are included in each message. You are responsible for all electronic mail originating from your user ID, therefore:

a) Unauthorized attempts to access another person's E mail or similar electronic communications or to use another's name, E mail or computer address or workstation to send E mail or similar electronic communications is prohibited and may subject the individual to disciplinary action.
b) All users must understand that the school cannot guarantee the privacy or confidentiality of electronic documents and any messages that are confidential as a matter of law should not be communicated over E mail.
c) The school reserves the right to access E mail to retrieve school information and records, to engage in routine computer maintenance and housekeeping, to carry out internal investigations, and/or to disclose messages, data or files to law enforcement authorities.
d) Any information contained on a school computer's hard drive or computer disks which were purchased by the school are considered the property of the school.
e) Forgery (or attempted forgery) of electronic mail is prohibited.
f) Attempts to send or sending harassing, obscene and/or other threatening e mail to another user are prohibited.
g) Attempts to send or sending unsolicited junk mail, "for profit" messages or chain letters are prohibited.

6) Security

Security on any computer system is a high priority, especially when the system involves many users. Never use another person's information to log onto the system. If you feel you can identify a security problem, you must notify a teacher or administrator. Do not demonstrate the problem to other users. Do not reveal your account password to anyone. Users are responsible for any misuse of their account that is due to their own negligence. Users are responsible for reporting unauthorized use of their account to a teacher or administrator.

7) Updating Your User Information

If any information on your account changes, (e.g., telephone number, location, home address) it is your responsibility to notify a teacher or administrator.

8) Services

St. Francis School makes no warranties of any kind, whether expressed or implied, for the computer and Internet service it is providing and will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the system is at your own risk.
St. Francis School specifically denies any responsibility for the accuracy or quality of information obtained through use of the Internet.

SECTION THREE: ADOPTION

Catholic Schools Office of the Diocese of Erie Acceptable Use and Internet Safety Policy
Approved by the Catholic Schools Office of the Diocese of Erie, August 2, 2010 - Revised June, 2012

ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

Purpose: To emphasize the importance that schools encourage good digital citizenship amongst students and staff in their use of computers, the Internet and other network resources. These are supported in the instructional and operational programs that facilitate learning, teaching, and daily school operations through interpersonal communications and access to pertinent information, up-to-date research and collaboration.

A. Definitions
Artificial Intelligence (AI) is the ability of a digital or computer or computer-controlled machine to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

The term child pornography is defined under both federal and state law.
Child pornography under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
Child pornography under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

The term harmful to minors is defined under both federal and state law.
Harmful to minors under federal law, is any picture, image, graphic image file or other visual depiction that:
1. Taken as a whole, 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 lewd exhibition of the genitals
3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:
1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;
2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors;
3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.
Obscene is any material or performance, if:
1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;
2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure is a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

Vandalism is any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses. Vandalism also includes, but is not limited to, damage to hardware, software, protective ware, and all associated equipment.

B. Requirements

- The availability of access to electronic information does not imply endorsement by the school of the content, nor does the school guarantee the accuracy of information received. The school shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.
- The school shall not be responsible for any unauthorized charges or fees resulting from access to the Internet and technology resources.
- Computer and network use are privileges, not rights. The school or school system's computer and technology resources are the property of the school or school system. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the school's Internet, computers or technology resources, including personal files or any use of
- the school's Internet, computers or technology resources. The school or system reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The school or school system shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the school's Internet, computers and technology resources.
- All users are required to fully comply with this policy and immediately report any violations or suspicious activities to the school principal or his/her designee.

In addition to those materials stated in law and defined in this policy, the Diocese prohibits deliberate or violative access to Internet sites or materials that promote, depict, contain, or advocate defamation, lewdness, vulgarity or profanity, inappropriate behavioral actions, harassment, discrimination, intolerance or hate, gambling, illegal weapons, bullying, terrorism or drug use. The school or school system reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established policy, or the use of software and/or online server blocking. Specifically, the school or school system operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.

Upon request by staff, the principal or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.

Upon written request by the staff, the principal or designee may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use.

The school or school system shall make every effort to ensure that this resource is used responsibly by students and staff.

The Acceptable Use and Internet Safety Policy (Appendix 202.2A) is to be given to all who use the school or school system networks or technology. Faculty, staff and volunteers who use school or school system networks or school-owned equipment shall, prior to being given access or being issued equipment, sign user agreements (Appendix 202.2B) acknowledging awareness of the provisions of this policy, and awareness that the school or school system uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Students and their parent/guardian must each sign agreements. (Appendix 202.2C and Appendix 202.2D) prior to being given access or being issued equipment

The principal or designee shall be responsible for recommending technology and developing procedures used to determine whether the school's computers are being used for purposes prohibited by law or for accessing materials harmful to minors. The procedures shall include but not be limited to:
• Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography,

harmful to minors with respect to use by minors, or determined inappropriate for use by minors
• Maintaining and securing a usage log
• Monitoring online activities of minors.

The principal or designee shall develop and implement regulations that ensure students are educated on network etiquette and other appropriate online behavior including, but not limited to, interaction with others on social media websites and cyberbullying awareness.

Network and email accounts shall be used only by the authorized owner of the account for its approved purpose. All users shall respect the privacy of others using the system. It is important to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Users shall not reveal personal information to other users on the network, including chat rooms, emails, social networking websites, etc.

Internet safety measures shall effectively address the following:
• Control of access by minors to materials harmful to minors on the Internet and World Wide Web
• Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
• Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities
• Unauthorized disclosure, use, and dissemination of personal information regarding minors
• Restriction of minors' access to materials harmful to them.

Users are expected to act in a responsible, ethical and legal manner in accordance with this policy, accepted rules of network etiquette, and federal and state law. Specifically, the following are prohibited:
1. Facilitating illegal activity
2. Personal, commercial or for-profit purposes
3. Nonwork or non-school related work
4. Product advertisement or political lobbying
5. Bullying/Cyberbullying or harassment
6. Hate mail, discriminatory remarks, and offensive or inflammatory communication
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with existing policies within the Diocese
10. Language or profanity that is harmful to minors
11. Transmission of material likely to be offensive or objectionable to recipients
12. Intentional obtaining or modifying of files, passwords, and data belonging to other users
13. Impersonation of another user, anonymity, and pseudonyms
14. Fraudulent copying, communications, or modification of materials in violation of copyright laws
15. Loading or using of unauthorized games, programs, files, or other electronic media
16. Disruption of the work of other users
17. Destruction, modification, abuse or unauthorized access to network hardware, software and files
18. Accessing the Internet, school computers or other network resources without authorization
19. Disabling or bypassing the Internet blocking/filtering software without authorization
20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization
21. Quoting personal communications in a public forum without the consent of the original author
22. Disseminating unauthorized student information, including but not limited to first or last name, address, telephone number, email address, or picture as defined in student records policy
23. Creating or participating in chain letters or similar forms of broadcast mail
24. The misuse or abuse of Artificial Intelligence (AI).

Internet communications are not guaranteed to be private, and individuals who operate the system do have access to electronic data. Communications relating to or in support of illegal activities may be reported to the authorities. Staff assisting students in creating student email addresses must use non-descriptive identifiers (such as numbers instead of names).

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, these guidelines shall be followed:
• Employees and students shall not reveal their passwords to another individual.
• Users are not to use a computer that has been logged in under another student's or employee's name.
• Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the school or school system network shall be subject to fair use guidelines and applicable laws and regulations.

The school and/or school systems shall establish and maintain a website and shall develop and modify its web pages to present information about the school under the direction of the president/principal or designee. All users publishing content on the school websites shall comply with this and other applicable policies.

Users shall not copy or download information from school websites and disseminate such information on unauthorized web pages without written authorization from the building administrator or program supervisor.

The user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network, intentional deletion or damage to files or data belonging to others, copyright violations, and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings.

Failure to comply with this policy or inappropriate use of the Internet, in violation of this policy, result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.
C. Legal Ramifications
The school or school system shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the school's website, and by other appropriate methods. All employees, volunteers, students and their parents are required to receive a copy of the Acceptable Use and Internet Safety Policy (Appendix 202.2A) Faculty/Staff/Volunteer agreements (Appendix 202.2B) must be signed, as well as, Student agreements (Appendix 202.2C). Parental Consent Agreements (Appendix 202.2D) must be signed for all students under the age of 18.

Effective August 2019