ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR MERCYHURST PREP
EMPLOYEES AND VOLUNTEERS

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

Mercyhurst Preparatory School provides Internet access, other online services and a wide range of technologies to its employees. In addition, appropriate resources are provided to volunteers when necessary. Such resources offer a multitude of global resources that are intended to be used for educational and professional purposes in accordance with the mission statement of Mercyhurst Preparatory School. Our goal in providing these services is to enhance the educational development of our students. All those who use the information technology resources at Mercyhurst Preparatory School must comply with the written policies covering their use as well as the spirit and intent of those policies. It is an expectation that all who use these resources do so in a responsible, efficient, courteous and legal manner.

Acceptable uses of technology are devoted to activities that support teaching and learning. Faculty, staff and volunteers must know that the network and technology devices are property of Mercyhurst Preparatory School and as such, should not be considered private. All school Internet use is filtered and monitored.

It is the policy of Mercyhurst Prep 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.

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. This includes attempting to log in through another person's account or accessing another person's "private" files. These actions are illegal. It is recognized that colleagues often need to share work. There are shared directories for this purpose, and staff are encouraged to use these shared locations when they want to share a "non-private" file with others.
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) Political lobbying. Employees may express opinions on legislative measures, but engaging in fundraising or other political activity will be considered unacceptable.
g) 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. Any activity that intentionally obstructs or hinders network traffic, network resources or desktop security is prohibited.
h) Copying programs purchased by you onto the school's computers and/or the network systems, without the express, written consent of the school
i) Copying programs, licensed to the school, for personal use
j) Abusing and disrupting electronic equipment and/or systems
k) Accessing, reviewing, uploading, downloading, completing, storing, printing, posting, receiving, transmitting or distributing pornographic, obscene or sexually explicit material; obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language; materials that use language or images that are inappropriate in the education setting or disruptive to the educational process.

Appropriate use of the network & computing facilities includes those uses that support:
- Instruction
- Independent study
- Research
- Career or professional development activities
- Official work of the offices and departments of Mercyhurst Prep
- Necessary professional communications that facilitate school authorized programs
- Personal use by staff is allowed as long as it does not interfere with the educational process, is not illegal and is not in violation of the Acceptable Use and Internet Safety Policy.

2) 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 an 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 an administrator.

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 copyright 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 email messages which have the capacity to overload the computer resources. Disciplinary measures may be imposed for intentional overloading of school computer resources.

<div align="center">

SECTION TWO: INTERNET ACCESS

</div>

Internet access is available to employees, students and, when indicated, volunteers of Mercyhurst Prep. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

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 pornography, including 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.

The following 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.

<div align="center">

INTERNET ACCESS: TERMS AND CONDITIONS

</div>

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 organizations' networks 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, copyright 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 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) Conserve resources such as disk space or printing capacity.
d) All communications and information accessible via the network should be assumed to be private property.

4) Online Safety and Behavior
Mercyhurst Prep, 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 including:
a) Appropriate online behavior;
b) Interacting with other individuals on social networking websites and chat rooms;
c) Cyber bulling 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 (Email)
Whenever you send electronic mail, your username 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 other person's email or similar electronic communications or to use another's name, email, or computer address or workstation to send email 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 email.
c) The school reserves the right to access email 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 email to another user are prohibited.
g) Attempts to send or sending unsolicited junk mail, "for profit" messages or chain letters are prohibited.

Employees or volunteers of Mercyhurst Prep should limit email and texting to students to essential items that support the educational or extracurricular programs of the school. Language used should be professional at all times.

6) Updating Your User Information
If any information on your account changes, (e.g., telephone number, location, home address) it is your responsibility to notify an administrator.

7) Privacy
The information systems of Mercyhurst Preparatory School and the files that reside on the computers are the property of Mercyhurst Preparatory School. Therefore, there is only a limited expectation of privacy within the network. The school has the right to examine all data stored on computers or other technology devices that are the property of the school to ensure that all users are in compliance with these regulations.

Individuals should be aware that our computing systems do generate logs of the activities of users. Please be aware that any misuse (as outlined in this document) of the computing facilities will be referred to the appropriate supervisory personnel.

It should be noted that email is insecure and may be read by authorized information system management personnel when deemed necessary by the president, principal, or by local, state, or federal officials in any investigation concerning or relating to any illegal

activities conducted using the school system.

Routine maintenance and monitoring of electronic technologies, including the school network, may lead to a discovery that a user has violated this policy, another school policy, or the law.

8) Software Guidelines
Software may be purchased from specific curriculum budgets and/or the school technology budgets. However, *before purchasing software*, staff should consult with the Technology or iPad director. This helps to avoid duplication, allows us to order in the most economical way, allows for purchasing of interdisciplinary pieces of software, and ensures that the software purchased will be compatible with the hardware, network, and security programs in place.

In order to prevent conflicts with software, as well as to comply with software copyright laws, all software on Mercyhurst Preparatory School computers must be installed ONLY under the following conditions:
- the software is licensed by the school and the license is on file in the appropriate office
- the Technology or iPad Director has given approval for installation
- technology staff has been given enough advance notice to allow for testing compatibility and installation of the new software
- the actual installation is carried out by the technology staff

9) Web Publishing Guidelines
The World Wide Web is an incredibly powerful publishing tool. Pages posted to the Web have the potential for having a worldwide audience in a matter of seconds. Publishing on the Web is strongly encouraged. If you are considering posting to the Web yourself, or having students post to the Web, you should familiarize yourself with the following guidelines.

Any material posted for the global community should reflect the high educational standard of Mercyhurst Prep and be compatible with the mission and other guiding documents. All published pages and corresponding links stored on school servers must be related to the school's educational goals and objectives or related to school-sponsored activities.

Individual teachers should review students' material before publication. The quality and completeness of any published work should be such that both student and teacher are proud that it can reach a global audience. Teachers are encouraged to have colleagues review classroom projects or individual student work before publishing on the Web.

10) Safety Rules for Student Publication
- Pictures that include the heads of students should be posted only if parents have not requested that they not be posted. Photo authorization forms may be required. Consult the principal before posting.
- Use no full names of students, except with parent permission.
- Divulge no contact information (home addresses, email addresses, phone numbers) of students.

If you are posting a class project and wish to link to the work of each student or group of students, an alias that the student has chosen can be used to attribute their work or link to it.

11) School Web Presence
The school's website was established to provide a learning experience for employees and students and to provide a venue for communications with parents and the community. All website content must support and promote the school's mission, goals and strategic direction.

The school encourages all teachers to establish a web page that supports their classroom instruction. If a teacher establishes a web page, he or she is responsible for maintaining that page. All classroom and teacher web pages must be linked to the Mercyhurst Prep's website.

Students may create web pages as part of classroom activities with teacher supervision and approval of the Technology department. The classroom teacher will review and approve all student-produced Web content prior to its posting.

Non-instructional and extracurricular web pages are also encouraged. However, all content should support the school's mission, and Mercyhurst Prep is responsible for all official entities that comprise our online presence. All entities must afford full administrative privileges to Kristin Lynch, MPS Director of Online Services, who will be able to help ensure brand consistency and faithfulness to the mission. At no time should the Mercyhurst Prep name or its derivatives be used without the explicit permission of the school's president.

12) Guidelines for Employees/Volunteers' Personal Use of Social Networking
The decision to use online social networking for personal use is at the employee's/volunteer's discretion. The school does not affirmatively monitor employee use of non-school, online social networking tools if the employee is not using the school's electronic technologies; however, the school may take appropriate action when it becomes aware of, or suspects, conduct or communication on an on line social media site that adversely affects the workplace, or violates acceptable professional codes of ethics, the diocesan Code of Conduct or the Mercyhurst Prep Acceptable Use and Internet Safety Policy. These guidelines are for employees/volunteers engaging in social networking for personal use.
- When using your personal social networking sites, refrain from fraternization with students. Don't friend students on Facebook, for example.
- Ensure that social networking postings are appropriate for the public.

364.2

- Weigh whether a posting will put your effectiveness as an employee at risk.
- Use caution with regard to exaggeration, profanity, guesswork, copyrighted materials, legal conclusions and derogatory comments.
- Ensure compliance with data privacy laws and school policies. Employees will be held responsible for inappropriate disclosure, whether purposeful or inadvertent.
- Respect your coworkers and students. Do not discuss students, their families, or coworkers.
- Student images obtained from your employment with the school should not be included on personal social networking sites.
- If the public may consider your statements to be made in your capacity as a school employee, you may want to include "this posting is my own and does not represent the view of Mercyhurst Prep." An employee in a leadership role in the school, by virtue of his or her position, must consider whether personal thoughts he or she published will be attributed the school.
- Social media identifications, login identifications, and user names must not contain the school's name or logo without prior written permission from the school president, principal, or designee.

School Limitation of Liability

Mercyhurst Preparatory School makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the school will be error-free or without defect. The school will not be responsible for any damage users may suffer, including but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by the system or your errors or omissions. The school is not responsible for the accuracy or quality of the information obtained through or stored on the system. Mercyhurst Prep specifically denies any responsibility for the accuracy or quality of information obtained through use of the Internet. The school will not be responsible for obligation, financial, legal or other, arising through the unauthorized use of the system. Use of any information obtained via the system is at your own risk.

August 2017