COMPUTER/ONLINE SERVICES
(Student Acceptable Use and Internet Safety)

Statement of Purpose

Please read this document carefully. This is part of the student code of conduct. Therefore, this is a legally binding agreement indicating that by using any district technology resource, students have read the terms and conditions carefully and understand their significance. The details of this agreement reflect Board policy EDE.

The Milford Exempted Village School District Board of Education recognizes that an effective educational system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the Milford Exempted Village School District will use technology resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes just as individuals in workplaces and other real-life settings. The district's technology resources will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives. The district authorizes the use of digital resources approved by the department of curriculum and instruction. Privacy policies for digital resources are available on the district website.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.

Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited, whether made with a district or personal technological device. This includes, but is not limited to, use of proxies, https, special ports, third party applications, portable hotspots, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.

The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers.

Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district.

Staff makes reasonable efforts to become familiar with the Internet and to monitor, instruct and assist effectively.

Students are obligated to immediately report inappropriate or questionable content inadvertently viewed or accessed. Students shall report content to staff, and staff shall report the content through the designated support helpdesk.

Personal Responsibility

By using the network resources of the district, you are agreeing not only to follow the rules in this policy, but are agreeing to report any misuse of the network to a teacher or building principal. Misuse means any violation of this policy, Board policy, or any other use that is not included in the policy, but has the effect of harming another person or his or her property.

Acceptable Use

Any student enrolled in the district will have computer network and Internet access during the course of the school year only, except for district-sponsored summer programs.

By using any district technology resources, students, staff and guests acknowledge and understand the following regarding the use of the computer/network:

1. Computer use is not private. System managers have access to all messages relating to or in support of illegal activities, activities not in the best interest of the district, and such activities may be reported to the authorities.

2. All electronic data that passes through a district-owned computer or over the district's network is subject to monitoring and seizure and may be handed over to law enforcement officers. The district reserves the right to inspect files stored on any personally owned device that is permitted to directly connect to the district network. An individual designation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or district policy.

3. All electronic data created for administrative or instructional purposes under the Board-approved curriculum for a course or program is the property of the district.

4. The rules and regulations of online etiquette are subject to change by the administration. The student code of conduct rules are applicable in the online environment as well.

5. The user in whose name a computer account is issued is responsible for its proper use at all times. Users must log off the computer to conclude a session or lock the computer if stepping away. Users retain responsibility for the activity of anyone accessing the computer and/or network under their account. Users shall keep personal account information, home addresses and telephone numbers private. They shall use this system only under the login and password information issued to them by the district. Users shall not grant others access to a computer and/or the network under their login and password. If you believe your computer account has been compromised, contact the ~~helpdesk or~~ building principal immediately.

6. Computer systems and the district network shall be used only for purposes related to education.

7. Violation of this policy and agreement may result in the cancellation of user privileges and possible discipline under the student code of conduct.

8. Use of personal technology devices on school grounds, inside district vehicles, or remotely connecting to district resources via the Internet is also governed by this policy.

The Milford Exempted Village School District is providing access to its computer network and the Internet for educational purposes only. If you have doubt about whether a contemplated activity is educational, you should ask your teacher or building principal if a specific use is appropriate.

Guidelines and Procedures

The following guidelines and procedures shall be complied with by staff, students or community members who are specifically authorized to use the district's computers or online services.

1. Use appropriate language. Do not use profanity, obscenity or other language that may be offensive to other users. Illegal activities are strictly forbidden.

2. Do not reveal your personal home address or phone number or those of other students or colleagues.

3. Note that electronic mail (email) is not guaranteed to be private. Superintendent/Designee has access to all messages relating to or in support of illegal activities and such activities may be reported to the authorities.

4. Use of the computer and/or network is not for financial gain or for any commercial or illegal activity.

5. The network should not be used in such a way that it disrupts the use of the network by others.

6. All communications and information accessible via the network should be assumed to be property of the district.

7. Rules and regulations of online etiquette are subject to change by the administration.

8. The user in whose name an online service account is issued is responsible for its proper use at all times. Users shall keep personal account numbers and passwords private. They shall use this system only under the account numbers issued by the district.

9. The system shall be used only for purposes related to education or administration. Commercial, political and/or personal use of the system is strictly prohibited. The administration reserves the right to monitor any computer activity and online communications for improper use.

10. Users shall not use the system to encourage the use of drugs, alcohol, or tobacco nor shall they promote unethical practices or any activity prohibited by law or Board policy.

11. Users shall not view, download or transmit material that is threatening, obscene, disruptive or sexually explicit or that could be construed as harassment, intimidation, bullying or disparagment of others based on their race, color, national origin, ancestry, citizenship status, sex, sexual orientation, age, disability, religion, economic status, military status, political beliefs or any other personal or physical characteristics.

12. Copyrighted material may not be placed on the system without the author's permission.

13. Vandalism results in the cancellation of user privileges. Vandalism includes uploading/downloading any inappropriate material, creating computer viruses and/or any malicious attempt to harm or destroy equipment or materials or data of any other user.

14. Users shall not read other users' mail or files; they shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to read, delete, copy, modify or forge other users' mail.

15. Users are expected to keep messages brief and use appropriate language.

16. Users shall report any security problem or misuse of the network to the teacher, his/her immediate supervisor or building administrator.

Unacceptable Use

Among the uses that are considered unacceptable and which constitute a violation of this policy are the following:

1. violating or encouraging others to violate the law or Board policy;

2. revealing private information about yourself or others. Private information includes, but is not limited to, a person's password, Social Security number, credit card number or other confidential information that has the potential to harm you or others or to violate the law if shared with other persons;

3. uses that cause harm to others, that cause damage to their property, or malicious actions to damage the reputation of another;

4. uses that constitute defamation (i.e., harming another's reputation by lies), or that harass, threaten or bully others;

5. using profanity, obscenity or other language that may be offensive to other users;

6. uses that are for commercial transactions (i.e., buying or selling or making arrangements to buy or sell over the Internet);

7. use that causes disruption to the use of the computer and/or network by others or that disrupts the educational process of the district;

8. using the system to encourage the use of drugs, alcohol or tobacco;

9. viewing, downloading or transmitting material that is threatening, pornographic, obscene, disruptive, or sexually explicit or that could be construed as harassment or disparagement of others based on their race, national origin, citizenship status, gender, sexual orientation, age, disability, religion or political beliefs;

10. copying or placing copyrighted material or software on the system without the author's permission and/or in violation of law;

11. reading, deleting, copying or modifying other users' email or files without their permission or attempting to interfere with another user's ability to use technology resources;

12. using another person's password or some other identifier that misleads recipients into believing someone other than you is communicating or accessing the network or Internet;

13. "hacking," gaining, or attempting to gain unauthorized access to computers, servers, computer systems, internal networks, or external networks;

14. possession of "hacking" tools or other malware;

15. downloading and/or installing freeware or shareware programs without the approval of the Technology Department. This includes use of peer-to-peer file sharing programs;

16. possession of or uploading a worm, virus or other harmful form of programming onto the network or Internet;

17. plagiarizing copyrighted or non-copyrighted materials for personal gain, recognition, or as graded work;

18. using social network sites such as Facebook, Twitter, and others and/or forum sites and/or blog sites for the purpose of posting slanderous or otherwise harmful information, whether true or untrue, about the character and/or actions of the district's students or staff on district or personal technology equipment and

19. using instant messaging, text messaging, video messaging and Internet telephone services without the consent of your teacher, supervisor, or director.

Privacy

Network and Internet access is provided as a tool for your education. The district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the district and no user shall have any expectation of privacy regarding such materials, regardless of storage location.

Electronic Vandalism / Cheating

Electronic vandalism will result in disciplinary action ranging from cancellation of privileges, suspension/expulsion and prosecution. Electronic vandalism is defined as any malicious attempt to harm or destroy data of another user or equipment or any network connected to any of the Internet backbones.

Electronic cheating is defined as any attempt to access the data of another student for the benefit of academic gain. This includes, but is not limited to, the uploading or creation of computer viruses or spyware, erasing, deleting, or otherwise making the school's programs or networks unusable and includes theft or the damaging or defacing of equipment. The district may hold users (or their legal guardian) personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs incurred, and any costs incurred to return such services to their normal state.

Warranties/Indemnification

The Milford Exempted Village School District makes no warranties of any kind, either express or implied, in the connection with its provision of access to and use of its computer networks and the Internet provided under this policy and agreement. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his/her parent(s) or guardian(s) arising out of

the user's use of its computer networks or the Internet under this policy and agreement. The user takes full responsibility of his/her usage and agrees to indemnify and hold harmless the Milford Exempted Village School District and its Board members, administrators, teachers and staff from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agrees to cooperate with the Milford Exempted Village School District in the event of the initiation of an investigation into a user's use or his or her access to its computer network and Internet, whether that use is on a district computer or on another's outside the Milford Exempted Village School district's Network.

As this policy is part of the student code of conduct, students agree to follow the Milford Exempted Village School District Acceptable Use Policy. Should a student commit any violation or in any way misuse access to the Milford Exempted Village School District's computers, computer network, and/or Internet, access privileges may be revoked and disciplinary action may be taken against him/her as outlined in the applicable handbook or code of student conduct.

Revised: January 28, 2015
Revised: April 19, 2018

COMPUTER NETWORK STUDENT AGREEMENT

I hereby apply for a student-account on the District computer network:

Student Name: _____

Building: _____

Student Address: _____

City, State, Zip: _____

Student Phone Number: _____

I have read and I understand this computer policy and its guidelines and regulations and agree to abide by all of the rules and standards for acceptable use stated therein. I further state that all information provided for the creation of this account is truthful and accurate.

_____ _____

SIGNATURE DATE

PARENTAL RELEASE FORM
(for students under 18 years of age)

_____ _____

PARENT(S) NAME - PLEASE PRINT

_____

STUDENT'S NAME – PLEASE PRINT

I/We have read and understand the computer policy and its guidelines and regulations and we agree to its terms and conditions. We confirm our child's intentions to abide by the terms and conditions therein. We also agree to supervise our child's use of the computer network from home or outside of the classroom.

_____ _____

SIGNATURE DATE