Administrative Regulation
Milford Public Schools
Milford, CT

The following regulations and expectations apply to all employees enrolled in the Milford Public Schools. They are in support of Milford Board of Education policies:

4118.5 Acceptable Use of Computers and Technology (Certified/Non-Certified)
4118.4 Electronic Mail
6156.2 Use of Computers in Instruction

Employee use of District technology will be governed by Board Policy including Policy 4118.5, Acceptable Use of Computers and Technology (Certified/Non-Certified). Users will adhere to Board Policy as well as the following regulations in using district technology.

Internet/Intranet
Users will adhere to the following regulations in using district networks, Internet/Intranet and other technology.

- Use of technology must be in support of the educational goals and objectives and building and district management of the Milford Public Schools.
- Within classroom instruction, use of technology must be consistent with the curriculum and appropriate to the instructional needs, learning styles, abilities and developmental levels of the students. Employees will preview the materials and specific sites they require or recommend students access to determine the appropriateness of the material contained on the site.
- Where applicable, employees will instruct students in the appropriate and acceptable use of District technology and will monitor and oversee appropriate student usage in an effort to prevent exposure to pornographic, indecent or obscene images or materials, to prevent unauthorized access, including hacking, by students, to prevent the unauthorized disclosure, use or dissemination of personal information regarding minors in accordance with the Children's Internet Protection Act. In accordance with the district's acceptable computer and technology policies and regulations, and other applicable district policies, regulations, rules and/or guidelines, including curriculum guidelines, employees will be responsible to educate their students about safe and appropriate online behavior for minors including, but not limited to, the use of social networking sites, chats room, and cyber bullying awareness and response. Employee and student users will comply with all state, federal and local laws, including copyright laws and laws prohibiting harassment by computer.
- Users will not commit acts of vandalism; they may not interfere with the performance of any district hardware or software or with the performance of the Internet/Intranet. This includes, but is not limited to, physical damage to District technology, entering closed areas of the network and introducing computer

viruses. Users will not use tools, software, or hardware in an effort to bypass Internet filtering. Users will not install any software without express permission.

- Users will not destroy or interfere with the work or data of others.
- Users will not use another person's login information or password at any time.
- Users will not engage in commercial ventures, nor will they incur charges for services, products, or information without appropriate administrative permission.
- Users will not reveal personal information about themselves or others, including, but not limited to, the following: home address, telephone numbers, password, social security number or credit card number.
- Users will report security problems to the supervising administrator or Instructional Technology Director.
- Unless restricted by the Superintendent, incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users.
- Users are responsible for the use of their individual account and should take all reasonable precautions to prevent student users or unauthorized persons from accessing their account.
- Users will comply with the provisions of the Family Educational Rights and Privacy Act (FERPA) and not post any student's personally identifiable information online without permission required by FERPA.
- Employees will promptly report/refer students or others to their supervising administrator if they witness or become aware of violations of the District's Acceptable Use policy, regulations, and/or agreement.
- Employees will familiarize themselves with the District's Student Acceptable Use of Technology policy and regulations and take advantage of reasonable opportunities to instruct and review with students the standards for acceptable use and precautionary measures to be taken to maintain personal safety on line.

Milford Public Schools E-Mails and Instant Messaging

Users will adhere to the following regulations in using district email.

1. Users will use e-mail and instant message accounts in a responsible, ethical and legal manner at all times.
2. Users will rely upon e-mail to communicate information, and all users will be responsible for checking and reading messages daily.
3. Users will use appropriate language and will be considerate of other e-mail users and their privacy; they will not forward any personal information about themselves or anyone else. Personal information includes home and school addresses and home, cell and school phone numbers, as well as information related to personal choices and activities.
4. Users will respect the privacy of others and not read the mail or files of others without their permission. Copyright and licensing laws will not be intentionally violated.
5. Users will not engage in bulk posting to individuals or groups to overload the system (i.e., "spamming") as it is prohibited, participate in chain letters, engage in solicitation of any nature including but not limited those for commercial gain, charitable donations, or on behalf of organizations as well as illegal activities; including, but not limited to, pyramid schemes.
6. Users will not send messages that contain false, malicious, or misleading information which may be injurious to a person or a person's property.

7. Users will not use e-mail to disrupt the school environment; this includes, but is not limited to, harassing or bullying any individual or groups of individuals, sexting, and using profane, lewd, inflammatory, threatening or disrespectful language.
8. While e-mail will have basic password authentication, it is not confidential. Administration reserves the right to bypass individual passwords at any time to monitor e-mails as well as to retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages or conduct internal investigations of wrongful acts.
9. In order to keep district electronic mail systems secure, staff may not leave the terminal "signed on" when unattended and may not leave their password available in an obvious place near the terminal or share their password with anyone.
10. The district retains the right to review, store and disclose all information sent over the district electronic mail systems for any legally permissible reason including, but not limited to, determining whether the information is a public record, whether it contains information discoverable in litigation and to access district information in an employee's or student's absence.
11. Electronic records, including e-mails, may be subpoenaed. Employees should be aware that their files may be discoverable under Connecticut State public records laws. All users must be aware that all information on District networks is subject to the freedom of information laws.

Confidentiality
All users of the district's computer and means of Internet access shall maintain the confidentiality of student and personnel records. Reasonable measures to protect against unreasonable access shall be taken before confidential student and personnel information is placed onto a network.

Internet Safety
Each district computer with internet access shall have a filtering device that blocks entry to websites and visual depictions that are obscene, pornographic, or harmful or inappropriate for students as defined by the Children's Internet Protection Act and as determined by the Superintendent or his/her designee. The Superintendent, or his/her designee, may disable the use of such filtering devices for bona fide research or other lawful purpose.

The Superintendent, or his/her disignee may edit or remove any material that it believes may be unlawful, obscene, indecent, abusive, or otherwise harmful to the school community.

The Superintendent or his/her designee is authorized to draft supplemental rules or guidelines to further guide students and employees charged with educating students about appropriate and safe online behavior including, but not limited to, the use of social networking sites, chat rooms and education regarding cyber bullying awareness and response.

District Approved and Supervised Social Networking
Users participating and managing district approved and supervised Social Networking, including blogs and wikis, must comply with the following regulations, as well as comply with any guidelines for use put forth by administrators:
1. Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all such district-sponsored social media activity.
2. If an employee wishes to use a social media site, such as Facebook, to extend a classroom learning experience or to communicate meetings, activities, games, responsibilities,

announcements, etc., for a school-based club, a school-based activity, organization, or sports team, the employee must also comply with the following rules:

- The employee must seek and obtain the permission of his/her supervisor prior to setting up the site. The employee must set up the club, etc. as a group list which will be "closed and moderated."
- Members will not be established as "friends," but as members of the group list.
- Anyone who has access to the communications conveyed through the site may only gain access by the permission of the employee (e.g. teacher, administrator, supervisor or coach). Persons desiring to access the page may join only after the employee invites them and allows them to join.
- Parents shall be permitted to access any site that their child has been invited to join.
- Access to the site may only be permitted for educational purposes related to the classroom, club, activity, organization or team.
- The employee responsible for the site will monitor it regularly.
- The employee's supervisor shall be permitted access to any site established by the employee at any time.
- Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all such district-sponsored social media activity.

3. Employees will comply with all technology regulations including the confidentiality of student information.
4. Milford Public Schools reserves the right to monitor all District sponsored social networking activity; employees should have no expectation of privacy in any communication or post made by them through social media while using district computers, cellular telephones or other electronic data devices.
5. All posts on district-sponsored social media must comply with the Board of Education's policies concerning confidentiality, including the confidentiality of student information. If an employee is unsure about the confidential nature of information the employee is considering posting, the employee shall consult with his/her supervisor prior to making the post.
6. An employee may not link a district-sponsored social media site or webpage to any personal social media sites not sponsored by the school district.
7. An employee may not use district-sponsored social media communications for personal reasons including private financial gain, political, commercial, advertisement, and proselytizing or solicitation purposes.
8. An employee may not use district-sponsored social media communications in a manner that misrepresents personal views as those of the Board of Education, individual school or school district, or in a manner that could be construed as such.
9. All district-sponsored social networking sites will be treated as classroom spaces and be created and maintained in accordance with all school rules and Board of Education policies.

Use of Personal Technology by Personnel

Personnel engaging in personal online social networking must be aware that:

1. Employees will not mention, discuss or reference the Board of Education, the school district or its individual schools, programs or teams on personal social networking sites, unless the employee also states that the post is the personal communication of the employee of the school district and that the views posted are the employee's alone and do not represent the views of the school district or the Board of Education.

2. Employees will not mention other Board of Education employees or other members of the school community (e.g., parents or others) on personal social networking sites, without such individual's express consent.
3. Employees will not use the Board of Education's logo or trademarks on their personal posts. Please note that this prohibition extends to the use of logos or trademarks associated with individual schools, programs or teams of the school district.
4. All posts on personal social media must comply with the Board of Education's policies concerning confidentiality, including the confidentiality of student information. If an employee is unsure about the confidential nature of information the employee is considering posting, the employee shall consult with his/her supervisor prior to making the post.
5. Employees will maintain appropriate professional boundaries with students, parents, and colleagues. For example, it is not appropriate for a teacher or administrator to "friend" a student or his/her parent or guardian or otherwise establish special relationships with selected students through personal social media, and it is not appropriate for an employee to give students or parents access to personal postings unrelated to school.
6. Employees are required to comply with all Board of Education policies and procedures with respect to the use of computer equipment, networks or electronic devices when accessing social media sites. Employees are strictly prohibited from using District technology to view, access or engage in the use of personal networking sites. Employees are further prohibited from using personal electronic devices to view, access or engage in the use of personal social media sites during school.
7. The Board of Education reserves the right to monitor all employee use of district computers and other electronic devices, including employee blogging and social networking activity. An employee should have no expectation of personal privacy in any personal communication or post made through social media while using district computers, cellular telephones or other electronic data devices.
8. Employees are individually responsible for their personal posts on social media. Employees may be sued by other employees, parents or others, and any individual that views an employee's social media posts as defamatory, pornographic, proprietary, harassing, libelous or creating a hostile work environment. As such activities are outside the scope of employment, employees may be personally liable for such claims.
9. All Board of Education policies that regulate off-duty conduct apply to social media activity including, but not limited to, policies related to public trust, illegal harassment, code of conduct and protecting confidential information. Accordingly, employees may be subject to disciplinary action for conduct that violates Board policies or standards for off-duty conduct in accord with the appropriate collective bargaining and District policy.
10. An employee may not link a personal social media site or webpage to the Board of Education's website or the websites of individual schools, programs or teams; or post Board of Education material on a social media site or webpage without written permission of his/her supervisor.

Personal Network Devices and Cellular Telephones

Users who introduce portable devices (wireless included) to the Milford Public Schools Network must comply with the following regulations, as well as comply with any guidelines for use put forth by administrators:

1. Users may introduce portable devices to the network including, but not limited to, wireless cell phones, wireless tablets and personal laptops
2. Users will agree to abide by all terms of the policies and regulations governing acceptable computer network use. The use of storage devices, i.e. thumb drives, is permissible by both

students and staff. Their use is limited to the transfer of school related work. All portable storage devices may be scanned for viruses before use.

3. Users may not use portable devices to disrupt the school environment; this includes, but is not limited to, harassing or cyber bullying any individual or groups of individuals as well as sexting and using profane, lewd, inflammatory, threatening or disrespectful language.
4. Users may not use portable devices on District networks for operating a personal business, sending or receiving chain letters, images, or advertisements, soliciting students or staff for any reason including but not limited to solicitation for commercial gain, charitable donations, or on behalf of organizations, or for engaging in illegal activities.
5. The district's computer network is considered a limited forum enabling the restriction of speech for valid educational reasons. For safety purposes the district employs both Internet filters and firewalls.

DISCLAIMER OF LIABILITY FOR EMPLOYEES PERSONAL USE OF TECHNOLOGY
While the Board is responsible for enforcing the operation of the technology protection measures during use of its computers, networks and other District technology, the Board expressly disclaims responsibility for imposing content filters, blocking lists , or monitoring of its employees personal technology or social media. All District employees who use personal technology and social media shall assume all risks associated with the use of personal technology and social media whether such use occurs on or off school grounds or during a school activity or event. The Board strongly encourages its employees to use personal technology responsibly at all times and to take into consideration the impact of such use on students, the school, and the school district as it relates to the employees' professional responsibilities and obligations.

Violation of Acceptable Use Regulations
The District will cooperate fully with local, state, or federal officials in any investigation concerning/relating to any illegal activities conducted through, by or using District computers, networks, Internet or other technology. The District reserves the right to additionally cooperate in investigations involving illegal personal technology usage by employees where such personal use impacts employees' ability to perform their jobs, is detrimental to student welfare or otherwise impacts the Board or school district.

Employees, who violate the Regulations within this document as well as the related policies, are subject to disciplinary action including termination of employment consistent with appropriate collective bargaining and District policy, state and federal law.

Acceptable Use of Computers and Technology Agreement
To ensure that only authorized personnel **who understand the bounds of permitted use will have access to the District technology, all users are required to sign an** Acceptable Use of Computers and Technology Agreement **acknowledg**ing **that he/she has read these regulations and expectations in addition to the related policies** and agrees to accept and abide by them in their entirety including those provisions related to monitoring, confidentiality and disclosure of records**.** The acknowledgment form will be retained in the employee's personnel file.

<u>District Responsibilities</u>
The Milford Board of Education makes every attempt to keep student access to the Internet safe. Access to the Internet is provided through the Connecticut Education Network (CEN) and is filtered. Filtered means that all content available to all those using the District's networks has been screened to eliminate content not deemed appropriate for a school environment. The filtering is accomplished with CEN as well as local filters. These filters are required by the

Children's Internet Protection Act and are a "best effort" attempt to keep our children safe. The Board recognizes that given the scope of the Internet, the filters may not restrict access to all controversial or potentially inappropriate material. The possibility of accessing such material does not mean that the Board endorses such content or consents to the accessing of such material. The Board is not responsible for Internet content which bypasses the filtering.

The District makes no warranties of any kind, expressed or implied, that the functions or the services provided by or through the District networks will be error-free or without defect. The Board specifically denies any responsibility for the accuracy or quality of information obtained via the Internet. Users access the Internet at their own risk and are responsible for checking the accuracy and quality of information. All provisions of this policy are subordinate to local, state and federal statutes.

The Superintendent or his/her designee shall be responsible for overseeing the implementation of these regulations and the accompanying related policies and for advising the Board of the need for any further amendments or revisions to policy/regulations. The Superintendent or his/her designee may develop additional administrative procedures/rules governing the day-to-day management and operations of the school district's computer system as long as they are consistent with the Board's policy/rules. The Superintendent may delegate specific responsibilities to building principals and others as he/she deems appropriate.

The District will not be responsible for any damages suffered by any user, including but not limited to loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions.

The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to the District's computer network or the Internet by employees. Employees may be held personally financially responsible for loss of or damage to, District's computers, its networks or other District technologies caused by employee's illegal or unacceptable use.

The Superintendent and the School Principals shall annually remind staff members and orient new staff members concerning the importance of maintaining proper decorum in the on-line, digital world as well as in person. Employees must conduct themselves in ways that do not distract from or disrupt the educational process.

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

Parental Notification and Responsibility

The District will notify parents about the District network and the policies governing its use. Parents must sign an agreement to allow their student to have use and have access to District computers, networks, the Internet and other District technology. Parents may request alternative computer activities for their child (ren) that does not require Internet access. A restricted use computer can be made available to network services without Internet access.

Parents have the right at any time to investigate the contents of their child(ren)'s files. Parents have the right to request the termination of their child(ren)'s individual account at any time.

Parents will be held financially responsible for any unauthorized costs incurred by their child(ren) in the use of District computers, networks or technologies, as well as monetary

damages incurred by the District resulting from the loss of, damage to, or the improper or illegal use by their child(ren) of the District's computers, its networks or other District technologies.

Monitoring

All computers, including all hardware and software and all electronic files and communications stored on or transmitted by District technology are the property of the District. All files stored on District networks or on District technology remain the property of the District and no user shall have any expectation of privacy regarding such material.

The District reserves the right to review, store and disclose all information sent or received through or stored on District computers, networks, the Internet or other District technology for any legally permissible reason, including but not limited to determining whether the information is a public record, whether it contains information discoverable in litigation and to access District information in an employee's absence, and to monitor compliance with this policy. The Board may edit or remove any material that it believes may be unlawful, obscene, indecent, abusive or otherwise harmful to the school community.

Employees will monitor student online behavior in accordance with district acceptable use of computers and technology policies, and regulations and all other applicable guidelines in order to promote the safe and appropriate use of technology by district students.

Users and guest users shall have no expectation of privacy in the use of or access to the District computers, networks, the Internet or other technology.

Copyright and Plagiarism

District policies on copyright will govern the use of material accessed through the District system. Teachers/employees will instruct students to respect copyright laws and to request permission for the use of copyrighted materials when appropriate.

District policies on plagiarism will govern use of material accessed through the District system. Teachers/employees will instruct students in appropriate research and citation practices.

Board of Education Reviewed: January 9, 2012