NEW MILFORD BOARD OF EDUCATION
New Milford Public Schools
50 East Street
New Milford, Connecticut 06776

POLICY SUB-COMMITTEE
MEETING NOTICE

DATE:	**December 6, 2022**
TIME:	**6:45 P.M.**
PLACE:	**Sarah Noble Intermediate School Library Media Center**

AGENDA

New Milford Public Schools Mission Statement

The mission of the New Milford Public Schools, a collaborative partnership of students, educators, family, and community, is to prepare each and every student to compete and excel in an ever-changing world, embrace challenges with vigor, respect and appreciate the worth of every human being, and contribute to society by providing effective instruction and dynamic curriculum, offering a wide range of valuable experiences, and inspiring students to pursue their dreams and aspirations.

1. **Call to Order**
2. **Public Comment**
   An individual may address the Board concerning any item on the agenda for the meeting subject to the following provisions:
   A. A three-minute time limit may be allocated to each speaker with a maximum of twenty minutes being set aside per meeting. The Board may, by a majority vote, cancel or adjust these time limits.
   B. If a member of the public comments about the performance of an employee or a Board member, whether positive, negative, or neutral, and whether named or not, the Board shall not respond to such comments unless the topic is an explicit item on the agenda and the employee or the Board member has been provided with the requisite notice and due process required by law. Similarly, in accordance with federal law pertaining to student confidentiality, the Board shall not respond to or otherwise discuss any comments that might be made pertaining to students.
3. **Discussion and Possible Action**
   A. Policies for First Review:
      1. 4118.6 Employee Use of the District's Computer Systems and Electronic Communications
      2. 5131.9 Student Use of the District's Computer Systems and Internet Safety
4. **Items of Information**
   A. Regulations:
      1. 4118.6R Administrative Regulation Regarding Employee Use of the District's Computer Systems and Electronic Communications
      2. 5131.9R Administrative Regulation Regarding Student Use of the District's Computer Systems and Internet Safety
   B. Audit of 5000 and 6000 Policy Series
5. **Public Comment**
   An individual may address the Board concerning any item on the agenda for the meeting subject to the following provisions:
   A. A three-minute time limit may be allocated to each speaker with a maximum of twenty minutes being set aside per meeting. The Board may, by a majority vote, cancel or adjust these time limits.
   B. If a member of the public comments about the performance of an employee or a Board member, whether positive, negative, or neutral, and whether named or not, the Board shall not respond to such comments unless the topic is an explicit item on the agenda and the employee or the Board

member has been provided with the requisite notice and due process required by law. Similarly, in accordance with federal law pertaining to student confidentiality, the Board shall not respond to or otherwise discuss any comments that might be made pertaining to students.

6. Adjourn

Sub-Committee Members: **Olga I. Rella, Chairperson**
Tammy McInerney
Leslie Sarich
Keith A. Swanhall, Jr.

Alternates: **Brian McCauley**
Eric Hansell

Note from Shipman & Goodwin:
Employee Use of the District's Computer Systems (15v13) (September 2022 Revision) We have revised this policy and the accompanying regulations to make technical edits to better reflect current composition of district computer networks and electronic messaging systems.

Series 4000 Personnel NEW # 4118.6

EMPLOYEE USE OF THE DISTRICT'S COMPUTER SYSTEMS AND ELECTRONIC COMMUNICATIONS

Computers, computer networks, electronic devices, Internet access, and electronic messaging systems are effective and important technological resources. The New Milford Board of Education (the "Board") has installed computers and a computer network(s), including Internet access and electronic messaging systems**,** on Board premises and may provide other electronic devices that can access the network(s) and/or have the ability to send and receive messages with an operating system or network communication framework. Devices include but are not limited to personal computing devices, cellular phones, Smartphones, network access devices, radios, personal cassette players, CD players, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices. Electronic messaging systems include mobile, chat, and instant message; cloud collaboration platforms, including internal chat, peer-to-peer messaging systems, and draft email message transfer; and products that have the ability to create duration-based or subjective removal of content, such as Snapchat, and security focused platforms, such as Signal. The Board's computers, computer networks, electronic devices, Internet access, and electronic messaging systems are referred to collectively as "the computer systems" and are provided in order to enhance both the educational opportunities for our students and the business operations of the district.

These computer systems are business and educational tools. As such, they are made available to Board employees for business and education-related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such computer systems are used for appropriate business and education-related purposes.

In accordance with applicable laws and the Administrative Regulations associated with this Policy, the system administrator and others managing the computer systems may access electronic messaging systems (including email) or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of electronic messaging systems (including email), messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using

social networking sites, including but not limited to, Twitter, Facebook, LinkedIn, Instagram and YouTube.

Incidental personal use of the computer systems may be permitted solely for the purpose of email transmissions and access to the Internet on a limited, occasional basis. Such incidental personal use of the computer systems, however, is subject to all rules, including monitoring of all such use, as the Superintendent may establish through regulation. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities.

Users should not have any expectation of personal privacy in the use of the computer system or other electronic devices that access the computer system. Use of the computer system represents an employee's acknowledgement that the employee has read and understands this policy and any applicable regulations in their entirety, including the provisions regarding monitoring and review of computer activity.

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250

Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

Policy adopted:

NEW MILFORD PUBLIC SCHOOLS
New Milford, Connecticut

Note from Shipman & Goodwin:
Student Use of the District's Computer Systems (15v13) (September 2022 Revision) We have revised this policy and the accompanying regulations to make technical edits to better reflect current composition of district computer networks and electronic messaging systems.

Series 5000 Students NEW # 5131.9

STUDENT USE OF THE DISTRICT'S COMPUTER SYSTEMS AND INTERNET SAFETY

Computers, computer networks, electronic devices, Internet access, and electronic messaging systems are effective and important technological resources. The New Milford Board of Education (the "Board") has installed computers and a computer network(s), including Internet access and electronic messaging systems on Board premises and may provide other electronic devices that can access the network(s) and/or have the ability to send and receive messages with an operating system or network communication framework. Devices include but are not limited to personal computing devices, cellular phones, Smartphones, network access devices, radios, personal cassette players, CD players, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices. Electronic messaging systems include mobile, chat, and instant message; cloud collaboration platforms, including internal chat, peer-to-peer messaging systems, and draft email message transfer; and products that have the ability to create duration-based or subjective removal of content, such as Snapchat, and security focused platforms, such as Signal. The Board's computers, computer network, electronic devices, Internet access, and electronic messaging systems are referred to collectively as "the computer systems" and are provided in order to enhance both the educational opportunities for our students and the business operations of the district.

These computer systems are business and educational tools. As such, they are made available to students in the district for education-related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such computer systems are used by students solely for education-related purposes. The Board will educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Additionally, the Board will implement a technology protection measure to block or filter Internet access to visual depictions that contain material that is obscene or obscene as to minors or contains child pornography, and ensure that such filtering technology is operative during computer use by minor students to the extent practicable when such students are using Board-owned computers or devices and Board-provided Internet access.

As the owner of the computer systems, the Board reserves the right to monitor the use of the district's computers and computer systems.

Legal References:

Conn. Gen. Stat. § 10-221

Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. §§ 2510 through 2520

Children's Internet Protection Act, Pub. L. 106-554, codified at 47 U.S.C. § 254(h)

No Child Left Behind Act of 2001, Pub. L. 107-110, codified at 20 U.S.C. § 6777

Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 U.S.C. § 254(h)(5)(B)(iii)

Policy adopted:

NEW MILFORD PUBLIC SCHOOLS
New Milford, Connecticut

Note from Shipman & Goodwin:
Employee Use of the District's Computer Systems (15v13) (September 2022 Revision) We have revised this policy and the accompanying regulations to make technical edits to better reflect current composition of district computer networks and electronic messaging systems.

Series 4000 Personnel **NEW # 4118.6R**

ADMINISTRATIVE REGULATION REGARDING EMPLOYEE USE OF THE DISTRICT'S COMPUTER SYSTEMS AND ELECTRONIC COMMUNICATIONS

Introduction

Computers, computer networks, electronic devices, Internet access, and electronic messaging systems are effective and important technological resources. The Board of Education (the "Board") has installed computers and a computer network(s), including Internet access and electronic messaging systems, on Board premises and may provide electronic devices that can access the network(s) and/or have the ability to send and receive messages with an operating system or network communication framework. Devices include but are not limited to personal computing devices, cellular phones,, Smartphones, network access devices, radios, personal cassette players, CD players, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices. Electronic messaging systems include mobile, chat, and instant message; cloud collaboration platforms, including internal chat, peer-to-peer messaging systems, and draft email message transfer; and products that have the ability to create duration-based or subjective removal of content, such as Snapchat, and security focused platforms, such as Signal. The Board's computers, computer networks, electronic devices, Internet access, and electronic messaging systems are referred to collectively as "the computer systems" and are provided in order electronic devices, to enhance the educational and business operations of the district. In these regulations, the computers, computer network, electronic devices, Internet access and email system are referred to collectively as "the computer systems."

These computer systems are business and educational tools. As such, they are being made available to employees of the district for district-related educational and business purposes. *All users of the computer systems must restrict themselves to appropriate district-related educational and business purposes*. Incidental personal use of the computer systems may be permitted solely for the purpose of email transmissions and similar communications, including access to the Internet on a limited, occasional basis. Such incidental personal use of the computer systems is subject to all rules, including monitoring of all such use, set out in these regulations. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities.

These computer systems are expensive to install, own and maintain. Unfortunately, these computer systems can be misused in a variety of ways, some of which are innocent and others deliberate. Therefore, in order to maximize the benefits of these technologies to the

district, our employees and all our students, this regulation shall govern *all* use of these computer systems.

Monitoring

It is important for all users of these computer systems to understand that the Board, as the owner of the computer systems, reserves the right to monitor the use of the computer systems to ensure that they are being used in accordance with these regulations. The Board intends to monitor in a limited fashion, but will do so as needed to ensure that the systems are being used appropriately for district-related educational and business purposes and to maximize utilization of the systems for such business and educational purposes. The Superintendent reserves the right to eliminate personal use of the district's computer systems by any or all employees at any time.

The system administrator and others managing the computer systems may access electronic messaging systems (including email) or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including, but not limited to, Twitter, Facebook, LinkedIn, Instagram and YouTube.

Notwithstanding the above and in accordance with state law, the Board may not: (1) request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing a personal online account; (2) request or require that an employee authenticate or access a personal online account in the presence of a Board representative; or (3) require that an employee invite a supervisor employed by the Board or accept an invitation from a supervisor employed by the Board to join a group affiliated with any personal online account of the employee. However, the Board may request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing (1) any account or service provided by the Board or by virtue of the employee's employment relationship with the Board or that the employee uses for the Board's business purposes, or (2) any electronic communications device supplied or paid for, in whole or in part, by the Board.

In accordance with applicable law, the Board maintains the right to require an employee to allow the Board to access the employee's personal online account, without disclosing the user name and password, password or other authentication means for accessing such personal online account, for the purpose of:

(A) Conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee's personal online account; or

(B) Conducting an investigation based on the receipt of specific information about an employee's unauthorized transfer of the Board's proprietary information, confidential information or financial data to or from a personal online account operated by an employee or other source.

For purposes of these Administrative Regulations, "personal online account" means any online account that is used by an employee exclusively for personal purposes and unrelated to any business purpose of the Board, including, but not limited to, electronic mail, social media and retail-based Internet web sites. "Personal online account" does not include any account created, maintained, used or accessed by an employee for a business purpose of the Board.

Why Monitor?

The computer systems are expensive for the Board to install, operate and maintain. For that reason alone it is necessary to prevent misuse of the computer systems. However, there are other equally important reasons why the Board intends to monitor the use of these computer systems, reasons that support its efforts to maintain a comfortable and pleasant work environment for all employees.

These computer systems can be used for improper, and even illegal, purposes. Experience by other operators of such computer systems has shown that they can be used for such wrongful purposes as sexual harassment, intimidation of co-workers, threatening of co-workers, breaches of confidentiality, copyright infringement and the like.

Monitoring will also allow the Board to continually reassess the utility of the computer systems, and whenever appropriate, make such changes to the computer systems as it deems fit. Thus, the Board monitoring should serve to increase the value of the system to the district on an ongoing basis.

Privacy Issues

Employees must understand that the Board has reserved the right to conduct monitoring of these computer systems and can do so *despite* the assignment to individual employees of passwords for system security. Any password systems implemented by the district are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user.

The system's security aspects, message delete function and personal passwords can be bypassed for monitoring purposes.

Therefore, *employees must be aware that they should not have any expectation of personal privacy in the use of these computer systems*. This provision applies to any and all uses of the district's computer systems and electronic devices that access same, including any incidental personal use permitted in accordance with these regulations.

Use of the computer system represents an employee's acknowledgement that the employee has read and understands these regulations and any applicable policy in their entirety, including the provisions regarding monitoring and review of computer activity.

Prohibited Uses

Inappropriate use of district computer systems is expressly prohibited, including, but not limited to, the following:

- Sending any form of solicitation not directly related to the business of the Board of Education;
- Sending any form of slanderous, harassing, threatening, or intimidating message, at any time, to any person (such communications *may* also be a *crime*);
- Gaining or seeking to gain unauthorized access to computer systems;
- Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from supervisory personnel;
- Sending any message that breaches the Board's confidentiality requirements, including the confidentiality rights of students;
- Sending any copyrighted material over the system;
- Sending messages for any purpose prohibited by law;
- Transmission or receipt of inappropriate email communications or accessing inappropriate information on the Internet, including vulgar, lewd or obscene words or pictures;
- Using computer systems for any purposes, or in any manner, other than those permitted under these regulations;
- Using social networking sites such as Facebook, Twitter, LinkedIn, Instagram and YouTube in a manner that violates the Board's Social Networking policy.

[If the Board does not have a formal social networking policy, the last bullet may be revised as follows:

- **Using social networking sites such as Facebook, Twitter, LinkedIn, Instagram and YouTube in a manner that disrupts or undermines the effective operation of the school district; is used to engage in harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate communications; creates a hostile work environment; breaches confidentiality obligations of school district employees; or violates the law, Board policies and/or the other school rules and regulations.]**

In addition, if a particular behavior or activity is generally prohibited by law and/or Board policy, use of these computer systems for the purpose of carrying out such activity and/or behavior is also prohibited.

Electronic Communications

The Board expects that all employees will comply with all applicable Board policies and standards of professional conduct when engaging in any form of electronic communication, including texting, using the district's computer system, or through the use of any electronic messaging system or electronic device or mobile device owned, leased, or used by the Board. As with any form of communication, the Board expects district personnel to exercise caution and appropriate judgment when using electronic communications with students, colleagues and other individuals in the context of fulfilling an employee's job-related responsibilities, including when engaging in remote teaching or use of a digital teaching platform.

Disciplinary Action

Misuse of these computer systems will not be tolerated and will result in disciplinary action up to and including termination of employment. Because no two situations are identical, the Board reserves the right to determine the appropriate discipline for any particular set of circumstances.

Complaints of Problems or Misuse

Anyone who is aware of problems with or misuse of these computer systems, or has a question regarding the appropriate use of the computer systems, should report this to a district administrator, supervisor or to _____.

Most importantly, the Board urges *any* employee who receives *any* harassing, threatening, intimidating or other improper message through the computer systems to report this immediately. It is the Board's policy that no employee should be required to tolerate such treatment, regardless of the identity of the sender of the message. *Please report these events!*

Implementation

This regulation is effective as of __/__/__.

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250

Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

Regulation adopted: NEW MILFORD PUBLIC SCHOOLS
New Milford, Connecticut

[Note: Although we have included this sample notice in our model policy documents for the convenience of our Board of Education clients, the notice does not need to be approved as a Board policy].

NOTICE REGARDING ELECTRONIC MONITORING

[To be posted in a conspicuous place readily available for viewing by employees]

In accordance with the provisions of Connecticut General Statutes Section 31-48d, the Board of Education hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the Board may not actually engage in the use of electronic monitoring, it reserves the right to do so as the Board and/or the Administration deem appropriate in their discretion, consistent with the provisions set forth in this Notice.

"Electronic monitoring," as defined by Connecticut General Statutes Section 31-48d, means the collection of information on the Board's premises concerning employees' activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the Board's premises which are open to the public, or (B) which is prohibited under other state or federal law.

The following specific types of electronic monitoring may be used by the Board in its workplaces: **[modify as appropriate for the school district in question]**

- Monitoring of electronic messaging systems (including email) and other components of the Board's computer systems, including monitoring of electronic devices such personal computing devices, cellular phones, Smartphones, network access devices, radios, personal cassette players, CD players, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices that access the computer systems, for compliance with the Board's policies and regulations concerning use of such systems.

- Video and/or audio surveillance within school buildings (other than in restrooms, locker rooms, lounges and other areas designed for the health or personal comfort of employees or for the safeguarding of their possessions), on school grounds and on school buses and other vehicles providing transportation to students and/or employees of the school system.

- Monitoring of employee usage of the school district's telephone systems.

- Monitoring of employees when employees are engaging in remote teaching or use of a digital teaching platform.

The law also provides that, where electronic monitoring may produce evidence of misconduct, the Board may use electronic monitoring without any prior notice when the Board has reasonable grounds to believe employees are engaged in conduct that (i) violates the law, (ii) violates the legal rights of the Board or other employees, or (iii) creates a hostile work environment.

Questions about electronic monitoring in the workplace should be directed to the Superintendent.

Legal References:

Connecticut General Statutes:
Section 31-48b
Section 31-48d

Note from Shipman & Goodwin:
Student Use of the District's Computer Systems (15v13) (September 2022 Revision) We have revised this policy and the accompanying regulations to make technical edits to better reflect current composition of district computer networks and electronic messaging systems.

Series 5000 Students **NEW # 5131.9R**

ADMINISTRATIVE REGULATION REGARDING STUDENT USE OF THE DISTRICT'S COMPUTER SYSTEMS AND INTERNET SAFETY

1. Introduction

a. *Access to District Computer Systems When Students Are Physically Present on School Property*

When students are physically present on school property, the Board is pleased to offer students access to the district's computers and computer networks, including access to electronic messaging systems (including email) and the Internet, as well as electronic devices (all of which will be referred to collectively as "computer systems"). Access to the school's computer systems will enable students to explore libraries, databases, websites, and bulletin boards while exchanging information with others. Such access is provided solely for education-related purposes. Use of the district's computer systems will be allowed only for students who act in a considerate and responsible manner in using such systems.

The Board of Education (the "Board") and the Administration believe in the educational value of such computer systems and recognize their potential to support our curriculum by expanding resources available for staff and student use. The Board's goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

These computer systems are expensive to purchase, install and maintain. As the property of the district, these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, students are required to adhere to a set of policies and procedures, as set forth in detail below, in conjunction with their use of the computer systems. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board's student discipline policy.

b. *Access to District Computer Systems When Students Are Engaged in Remote Learning*

The Board and the Administration recognize that technology is integral to the delivery of instruction if and when the district implements any form of digital or remote learning. The district may therefore provide students with remote access to some or all of the district's computer systems so that students may access the district's virtual learning environment. Such access, if granted, is provided solely for education-related purposes. Use of the district's computer systems will be allowed only for students who comply with district

policies and procedures concerning computer system use, and demonstrate the ability to use the computer systems in a considerate and responsible manner.

These computer systems are expensive to purchase, install and maintain. As the property of the district, these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, students will be required to adhere to a set of policies and procedures, as set forth in detail below, in conjunction with their use of the computer systems. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board's student discipline policy.

2. Definitions

Obscene – means any material or performance if, a) taken as a whole, it predominantly appeals to the prurient interest, b) it depicts or describes in a patently offensive way a prohibited sexual act and c) taken as a whole, it lacks serious literary, artistic, educational, political or scientific value.

Obscene as to minors - means any material or performance if it depicts a prohibited sexual act and, taken as a whole, it is harmful to minors.

For purposes of this section, "***harmful to minors***" means that quality of any description or representation, in whatever form, of a prohibited sexual act, when a) it predominantly appeals to the prurient, shameful or morbid interest of minors, b) it is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors, and c) taken as a whole, it lacks serious literary, artistic, educational, political or scientific value for minors.

For the purposes of this section, "***prohibited sexual act***" means erotic fondling, nude performance, sexual excitement, sado-masochistic abuse, masturbation or sexual intercourse.

Child pornography –means 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 -

(a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
(b) such visual depiction is a digital image, computer mage, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
(c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

3. Monitoring

Students are responsible for good behavior on school computer systems just as they are in a classroom or a school hallway. Communications on the computer systems are often public in nature and general school rules for behavior and communications apply. It is expected that users will comply with district standards and will act in a responsible and

legal manner, at all times in accordance with district standards, as well as with state and federal laws.

It is important that students and parents understand that the district, *as the owner of the computer systems, reserves the right to monitor and review* the use of these computer systems. The district intends to monitor and review in a limited fashion, but will do so as needed to ensure that the systems are being used for district-related educational purposes.

As part of the monitoring and reviewing process, the district will retain the capacity to bypass any individual password of a student or other user. *The system's security aspects, such as personal passwords and the message delete function for email, can be bypassed for these purposes*. The district's ability to monitor and review is not restricted or neutralized by these devices. The monitoring and reviewing process also includes, but is not limited to: oversight of Internet site access, the right to review electronic messages sent and received, the right to track students' access to blogs, electronic bulletin boards and chat rooms, and the right to review a student's data downloading and printing.

Therefore, all users must be aware that *they should not have any expectation of personal privacy in the use of these computer systems.*

4. Student Conduct

Students are permitted to use the district's computer systems for legitimate educational purposes. Personal use of district computer systems is expressly prohibited. Conduct which constitutes inappropriate use includes, but is not limited to the following:

- Sending any form of a harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);
- Gaining or seeking to gain unauthorized access to computer systems;
- Damaging computers, computer files, computer systems or computer networks;
- Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from a teacher or administrator;
- Using another person's password under any circumstances;
- Trespassing in or tampering with any other person's folders, work or files;
- Sending any message that breaches the district's confidentiality requirements, or the confidentiality of students;
- Sending any copyrighted material over the system;

- Using computer systems for any personal purpose, or in a manner that interferes with the district's educational programs;

- Accessing or attempting to access any material that is obscene, obscene as to minors, or contains child pornography, as defined above;

- Transmitting or receiving email communications or accessing information on the Internet for non-educational purposes;

- Cyberbullying;

- Accessing or attempting to access social networking sites (e.g., Facebook, Twitter, Instagram, Snapchat, TikTok, etc.) without a legitimate educational purpose.

In addition, as noted above, if a particular behavior or activity is generally prohibited by law, by Board policy or by school rules or regulations, use of these computer systems for the purpose of carrying out such behavior or activity is also prohibited.

Misuse of the computer systems, or violations of these policies and regulations, may result in loss of access to such computer systems as well as other disciplinary action, including suspension and/or expulsion, depending on the specific conduct.

Anyone who is aware of problems with, or misuse of, these computer systems, or has a question regarding the proper use of these computer systems, should report or discuss the issue with a teacher or the school principal immediately. Most importantly, the Board and the Administration urge *any* student who receives *any* harassing, threatening, intimidating or other improper message through the computer system to report this immediately. It is the Board's policy that no student should be required to tolerate such treatment, regardless of the identity of the sender of the message. *Please report these events!*

5. Internet Safety

The Administration will take measures: to assure the digital safety and security of students when using electronic messaging systems, email, chat rooms, distance learning platforms, and other forms of direct electronic communications; to prohibit unauthorized access, including "hacking" and other unlawful activities by minors online; to prohibit unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; to educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response; and to restrict students' access to online materials that are obscene or obscene as to minors or contain child pornography, to the extent practicable when students are using Board-owned computers or devices and Board-provided Internet access.

6. Student Use Agreement

Before being allowed to use the district's computer systems, students and/or their parents/guardians must sign a computer system use agreement, stating that they have read

and understood the district's policies and regulations regarding the use of its computer systems.

Legal References:

Conn. Gen. Stat. § 10-221

Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250 *et. seq*. (computer-related offenses)

Conn. Gen. Stat. § 53a-193 (definition of obscene and obscene as to minors)

18 U.S.C. § 2256 (definition of child pornography)

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. §§ 2510 through 2520

Children's Internet Protection Act, Pub. Law 106-554, codified at 47 U.S.C. § 254(h)

No Child Left Behind Act of 2001, Pub. L. 107-110, codified at 20 U.S.C. § 6777

Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 U.S.C. § 254(h)(5)(B)(iii)

Miller v. California, 413 U.S. 15 (1973) (definition of obscene)

Regulation adopted:

NEW MILFORD PUBLIC SCHOOLS
New Milford, Connecticut