# #9220.4
# Removal of Board Officers
**(formerly Board Member Removal from Office)**

~~Any officer of the Board, except the Treasurer, may be removed from office by a two-thirds (2/3) vote of the entire membership of the Board. The Chairperson shall select a temporary officer to act in that capacity for a period of time not to exceed six (6) weeks, during which time a special election for that office shall be held, as specified under the terms of Madison Board of Education Bylaw #9400. The newly elected officer shall serve out the term of the officer being replaced.~~

~~Date of Adoption: 3/7/95~~

~~Reference: Bylaw # 9220.3~~
~~Bylaw # 9400~~

It is the policy of the Madison Board of Education (the "Board") that officers of the Board will:

1. adhere to all Board policies, rules and regulations;
2. conduct themselves in a fair and impartial manner; and
3. carry out the duties of their respective offices in accordance with law.

An officer of the Board may be removed for cause by a ~~majority OR~~ 2/3 vote of the entire Board. A vote to remove a Board officer shall only take place at a regular meeting or a special meeting called for that purpose. "Cause," which means a reasonable ground for removal, includes, but is not limited to, any conduct that:

1. specifically relates to and affects the administration of the office in a manner deemed to be deleterious to Board operations;
2. negatively and directly affects the rights and interests of the public;
3. violates Board policies, rules and regulations; ~~or~~
4. interferes with the orderly and efficient operation of the Board; or
5. failure to serve as defined in Section 6.5 of the Madison Town Charter.~~.~~

## Procedures for Removal

The following procedures shall be used in lieu of any procedures set forth in Robert's Rules of Order with respect to any proposed action to remove or take other disciplinary action regarding an officer of the Board for cause:

1) The Board shall review the performance and/or conduct of an officer of the Board in open or executive session (as determined by the Board and the Board officer in accordance with the Freedom of Information Act) at a regular or special meeting of the Board, prior to initiating any action to remove or take other disciplinary action regarding a Board officer for cause.

2) If the Board determines as a result of such discussion that formal action is necessary, the Board shall provide the Board officer with:

   a) reasonable written notice of the Board's intent to consider removal or other disciplinary action, including the factual basis for the claimed "cause" for removal of the officer from office, with such notice to be provided after being authorized by ~~majority~~ a 2/3 vote of those Board members present and voting; and

   b) an informal opportunity to be heard by the Board regarding such possible removal or other disciplinary action, at which the Board officer shall have the right to be represented by counsel at the Board member's own expense and to present relevant evidence to the Board. The informal opportunity to be heard shall take place in open or executive session (as determined by the Board and the Board officer in accordance with the Freedom of Information Act) at a regular or special meeting of the Board.

3) Any action to remove or take other disciplinary action regarding a Board officer for cause following such informal hearing shall require an affirmative vote by ~~a majority~~ 2/3 of all members of the Board.

Service as a Board officer is a privilege, the purpose of which is to assist the Board in conducting its business in an appropriate, orderly and efficient manner. Therefore, any Board member serving as an officer shall have no legally protected right to continue in that position.

Legal References:

Connecticut General Statutes

10-218 Officers. Meetings.
10-220 Duties of boards of education.

*LaPointe v. Board of Education of the Town of Winchester*, 274 Conn. 806 (2005).

First Reading: May 9, 2023

# #4150
# Employee Use of the District's Computer Systems
## (formerly Acceptable Use of Computer equipment and Related Systems, Software and Networks)

Computers, computer networks, electronic devices, Internet access, and electronic messaging systems are effective and important technological resources. The Madison 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, copiers, Smartphones, work phones, network access devices, radios, 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 employees of the district for district-related educational and business purposes~~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.

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 Freedom of Information Act requests and 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

First Reading: May 9, 2023

# Regulation #4150
# Employee Use of District's Computer Systems

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, copiers, Smartphones, work phones, network access devices, radios, 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 IT Department personnel;
- Damaging equipment through careless handling, loss, or theft;
- 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;
- Storing personal or confidential information on the system;
- Transmission 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 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;
- Violating cybersecurity best practices through the sharing of passwords.

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 or its designee 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 the school principal.

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

# #4150
# Acceptable Use of Computer Equipment and Related Systems, Software and Networks

The Madison Board of Education provides computers, computer systems, software, electronic access privileges, and networks for students and staff to carry out the educational mission of the Board and to enhance the curriculum and learning opportunities for students and staff in an environment which ensures access to, and management of, up-to-date information and communication services. Responsible use of these systems and networks is expected of all staff.

The computers, computer systems, software, electronic access privileges, and networks are the property of the Madison Board of Education and are to be used only for those activities directly related to teaching, learning, and / or management by staff. The equipment, infrastructure, and software are not to be used for personal gain by any student or staff member.

The computers, computer systems, software, electronic access privileges, and networks provided by the Madison Board of Education shall not be modified or altered by individual users without the authorization of the Superintendent or his / her designee.

All users are hereby made aware that all information on the Madison Board of Education's computers, computer systems, software, , and networks are in the public domain, unless specifically protected by the Connecticut Freedom of Information Act. Users should not assume that any information accessed or stored on the computers, computer systems, or networks provided by the Madison Board of Education is private.

The Madison Board of Education reserves the right to bypass any or all individual or group passwords to determine the activity on any or all of the computers, computer systems, software, electronic access privileges, and networks.

All District computers remain under the control, custody and supervision of the district. The District reserves the right to monitor all computer network and Internet activity by employees, whether using district issued devices or accessing the Madison network via personally owned devices.

The Superintendent shall establish appropriate guidelines and procedures for responsible use of computer systems and devices, software, electronic access privileges, networks, and the internet provided by the Madison Board of Education. Employees are required to periodically sign an appropriate Network Use Agreement in order to access network resources. Employees who violate this policy may be subject to disciplinary action.

(cf. 5210: Accepted Use of Computers, Computer Systems, Software, Electronic Access Privileges, and Networks)

Legal Reference: Connecticut General Statutes
The Freedom of Information Act
53A-182B Harassment in the first degree
31-48d Employers engaged in electronic monitoring required to give prior notice to employees.

Date of Adoption: November 4, 1999
Date of Revision: November 7, 2006
Date of Revision: June 5, 2012

# #5210
# Student use of the District's Computer Systems and Internet Safety
**(formerly Acceptable Use of Computer Equipment and Related Systems, Software & Networks)**

Computers, computer networks, electronic devices, Internet access, and electronic messaging systems are effective and important technological resources. The Madison 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, 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)

First Reading: May 9, 2023

# Regulation #5210
# 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 image, 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 e-mail, 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 gain, 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 e-mail 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)

# #5210
# Acceptable Use of Computer equipment and Related Systems, Software & Networks

The Madison Board of Education provides computers, computer systems, software, electronic access privileges, and networks for students and staff to carry out the mission of the Board in an environment which ensures access to, and management of, up-to-date information and communication services. Responsible use of these systems and networks is expected of all students and staff.

The computers, computer systems, software, electronic access privileges, and networks are the property of the Madison Board of Education and are to be used only for those activities directly related to teaching, learning, and / or management by students and staff. The equipment, infrastructure, and software are not to be used for personal gain by any student or staff member.

The computers, computer systems, software, electronic access privileges, and networks provided by the Madison Board of Education shall not be modified or altered by individual users without the authorization of the Superintendent or his / her designee.

All users are hereby made aware that all information on the Madison Board of Education's computers, computer systems, software, and networks is in the public domain, unless specifically protected by the Connecticut Freedom of Information Act. Users should not assume that any information accessed or stored on the computers, computer systems, or networks provided by the Madison Board of Education is private.

The Madison Board of Education reserves the right to bypass any or all individual or group passwords to determine the activity on any or all of the computers, computer systems, software, electronic access privileges, and networks.

The Superintendent shall establish grade level appropriate guidelines and procedures for responsible use of computer systems and devices, software, electronic access privileges, networks, and the internet provided by the Madison Board of Education.

The district shall provide student education about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other individuals on social networking sites and in chat rooms. Parents are required to annually sign a grade level appropriate Network Use Agreement granting permission for their child to access network resources. Students who violate this policy will be subject to disciplinary action. The Superintendent shall propose and the Board of Education shall approve procedures and regulations to ensure that any student violating this policy is subjected to disciplinary action, and that any disciplinary actions imposed for similar violations are treated consistently.

Legal Reference: Conn. Gen. Stat. Sec. 10-221

(cf 4150: Accepted Use of Computers, Computer Systems, Software, Electronic Access Privileges, and Networks)

Date of Adoption: November 4, 1999
Date of Revision: August 16, 2005
Date of Revision: May 15, 2012

# #5090.9
# Use of Private Technology Devices by Students
**(formerly Electronic Communication Device)**

Students may possess privately-owned technological devices on school property and/or during school-sponsored activities, in accordance with the mandates of this policy and any applicable administrative regulations as may be developed by the Superintendent of Schools.

**Definitions**

Board Technology Resources

For the purposes of this policy, "Board technology resources" refers to the Madison Board of Education's (the "Board's") computers and instructional technologies; communications and data management systems; informational technologies and the Internet; and any other technology resources owned and/or used by the school district and accessible by students.

Privately-owned Technological Devices

For the purposes of this policy, "privately-owned technological devices" refers to, but is not limited to, privately-owned desktop computers, personal computing devices, cellular phones, Smartphones, network access devices, radios, personal audio players, ~~CD players~~, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices. ~~wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. These devices may include, but are not limited to, desktops, personal laptops, Smartphones, network access devices, Kindles, Nooks, cellular telephones, radios, personal audio players, I-Pads or other tablet computers, walkie-talkies, Blackberries, personal data assistants, I-Phones, Androids and other electronic signaling devices.~~

#5090.9(b)

**Use of Privately-Owned Technological Devices**

Privately-owned technological devices may not be used during instructional time, except as specifically permitted by instructional staff or unless necessary for a student to access the district's digital learning platform or otherwise engage in remote learning if remote learning has been authorized in accordance with applicable law.

On school property, at a school-sponsored activity, while in use for a remote learning activity if remote learning has been authorized in accordance with applicable law, or while being used to access or utilize Board technology resources, the use of any such device for an improper purpose is prohibited. Improper purposes include, but are not limited to:

- 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 Board technology resources;
- Damaging Board technology resources;
- Accessing or attempting to access any material that is obscene, obscene as to minors, or contains pornography;
- Cyberbullying;
- Using such device to violate any school rule, including the unauthorized recording (photographic, video, or audio) of another individual without the permission of the individual or a school staff member; or
- Taking any action prohibited by any Federal or State law.

#5090.9(c)

**Search of Privately-Owned Technological Devices**

A student's privately-owned technological device may be searched if the device is on Board property or in a student's possession at a school-sponsored activity and if there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school. Any such search shall be reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.

**Responsibility for Privately-owned Technological Devices**

Students are responsible for the safety and use of their privately-owned technological devices. If a privately-owned technological device is stolen, lost, or damaged while the device is on school property or during a school-sponsored activity, a report should be made to the building principal, who will investigate the loss in a manner consistent with procedures for stolen or damaged personal property. Students and parents should be aware that the Board is not liable for any privately-owned technological device that is stolen, lost, or damaged while at school or during a school-sponsored activity. For that reason, students are advised not to share or loan their privately-owned technological devices with other students.

**Disciplinary Action**

Misuse of the Board's technology resources and/or the use of privately-owned technological devices to access or utilize the Board's technology resources in an inappropriate manner or the use of such devices in any manner inconsistent with this policy will not be tolerated and will result in disciplinary action. For students, a violation of this policy may result in loss of access privileges, a prohibition on the use and/or possession of privately-owned technological devices on school property or at school-

sponsored activities, and/or suspension or expulsion in accordance with the Board's policies related to student discipline.

**Access to Board Technology Resources**

The Board may permit students, using their privately-owned technological devices, to access the Board's computers and instructional technologies; communications and data management systems; informational technologies and the Internet; and any other technology resources used by the school district and accessible by students. Students using privately-owned technological devices will agree to access the District's technology resources only through the designated Wi-Fi network. Additionally, it is the expectation of the Board that students who access these resources while using privately-owned technology devices will act at all times appropriately in ways ~~which~~ that are fully in accord with applicable policies concerning technology use as well as all local, state, and federal laws.

Through the publication and dissemination of this policy statement and others related to use of the Board's computer systems, as well as other instructional means, the Board educates students about the Board's expectations for technology users.

The Board's technology resources shall only be used to access educational information and to promote learning activities both at home and at school. Students are expected to act at all times appropriately in ways ~~which~~ that are fully in accord with applicable policies concerning technology use as well as all local, state, and federal laws when using the Board technology resources. Failure to do so will result in the consequences outlined herein and in other applicable policies (including, but not limited to, the Safe School Climate Plan, the Student Discipline Policy and the Use of Computers Policy).

Students must abide by the procedures outlined in this policy and all policies and applicable regulations outlined in the Board's computer use and other applicable policies. Students will be given specific information for log-on and access procedures for using

school accounts. No user may deviate from these log-on/access procedures. **Students are advised that the Board's network administrators have the capability to identify** **#5090.9(e)** **users and to monitor all privately-owned technological devices while they are logged on to the network.** Students must understand that the Board has reserved the right to conduct monitoring of Board technology resources and can do so *despite* the assignment to individual users of passwords for system security. Any password systems implemented by the Board 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, students should be aware that they should not have any expectation of personal privacy in the use of privately-owned technological devices to access Board technology resources. This provision applies to any and all uses of the Board's technology resources and any privately-owned technological devices that access the same.

**Harm to Board Technology Resources**

Any act by a student using a privately-owned technological device that harms the Board technology resources or otherwise interferes with or compromises the integrity of Board technology resources will be considered vandalism and will be subject to discipline and/or appropriate criminal or civil action.

**Closed Forum**

This policy shall not be construed to establish a public forum or a limited open forum.

Legal References:

Conn. Gen. Stat. § 10-233j

Conn. Gen. Stat. § 31-48d

Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250, *et seq.*

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 28 U.S.C. §§ 2510 through 2520

Date of Adoption: September 5, 1995
Date of Revision: October 15, 1996
Date of Revision December 1, 1998
Date of Revision: April 23, 2002
Date of Revision: June 1, 2010
Date of Revision: June 5, 2012
Date of Revision: October 15, 2013
Date of Revision: June 21, 2022

First Reading: May 9, 2023