

#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:

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

49
50 2) If the Board determines as a result of such discussion that formal action is
51 necessary, the Board shall provide the Board officer with:

52
53 a) reasonable written notice of the Board’s intent to consider removal or
54 other disciplinary action, including the factual basis for the claimed
55 “cause” for removal of the officer from office, with such notice to be
56 provided after being authorized by ~~majority~~ a 2/3 vote of those Board
57 members present and voting; and

58
59 b) an informal opportunity to be heard by the Board regarding such possible
60 removal or other disciplinary action, at which the Board officer shall have
61 the right to be represented by counsel at the Board member’s own expense
62 and to present relevant evidence to the Board. The informal opportunity
63 to be heard shall take place in open or executive session (as determined by
64 the Board and the Board officer in accordance with the Freedom of
65 Information Act) at a regular or special meeting of the Board.

66
67 3) Any action to remove or take other disciplinary action regarding a Board
68 officer for cause following such informal hearing shall require an affirmative
69 vote by ~~a majority~~ 2/3 of all members of the Board.

70
71 Service as a Board officer is a privilege, the purpose of which is to assist the Board in
72 conducting its business in an appropriate, orderly and efficient manner. Therefore, any
73 Board member serving as an officer shall have no legally protected right to continue in
74 that position.

75
76
77 Legal References:

78
79 Connecticut General Statutes

80 10-218 Officers. Meetings.

81 10-220 Duties of boards of education.

82
83 LaPointe v. Board of Education of the Town of Winchester, 274 Conn. 806 (2005).

84
85 First Reading: May 9, 2023

86 Second Reading: June 6, 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

34 electronic messaging systems (including email) or monitor activity on the computer system
35 or electronic devices accessing the computer systems at any time and for any reason or no
36 reason. Typical examples include when there is reason to suspect inappropriate conduct or
37 there is a problem with the computer systems needing correction. Further, the system
38 administrator and others managing the computer systems can access or monitor activity on
39 the systems despite the use of passwords by individual users, and can bypass such
40 passwords. In addition, review of electronic messaging systems (including email),
41 messages or information stored on the computer systems, which can be forensically
42 retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using
43 social networking sites.

44
45 Incidental personal use of the computer systems may be permitted solely for the purpose
46 of email transmissions and access to the Internet on a limited, occasional basis. Such
47 incidental personal use of the computer systems, however, is subject to all rules, including
48 Freedom of Information Act requests and monitoring of all such use, as the Superintendent
49 may establish through regulation. Moreover, any such incidental personal use shall not
50 interfere in any manner with work responsibilities.

51
52 **Users should not have any expectation of personal privacy in the use of the computer**
53 **system or other electronic devices that access the computer system. Use of the**
54 **computer system represents an employee’s acknowledgement that the employee has**
55 **read and understands this policy and any applicable regulations in their entirety,**
56 **including the provisions regarding monitoring and review of computer activity.**

57
58 Legal References:

- 59
60 Conn. Gen. Stat. § 31-40x
61 Conn. Gen. Stat. § 31-48d
62 Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250

63
64 Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

65
66 First Reading: May 9, 2023
67 Second Reading: June 6, 2023

Regulation #4150

Employee Use of District's Computer Systems

1
2
3
4 Introduction

5
6 Computers, computer networks, electronic devices, Internet access, and electronic
7 messaging systems are effective and important technological resources. The Board of
8 Education (the "Board") has installed computers and a computer network(s), including
9 Internet access and electronic messaging systems, on Board premises and may provide
10 electronic devices that can access the network(s) and/or have the ability to send and receive
11 messages with an operating system or network communication framework. Devices
12 include but are not limited to personal computing devices, cellular phones, copiers,
13 Smartphones, work phones, network access devices, radios, tablets, walkie-talkies,
14 personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic
15 signaling devices. Electronic messaging systems include mobile, chat, and instant
16 message; cloud collaboration platforms, including internal chat, peer-to-peer messaging
17 systems, and draft email message transfer; and products that have the ability to create
18 duration-based or subjective removal of content, such as Snapchat, and security focused
19 platforms, such as Signal. The Board's computers, computer networks, electronic devices,
20 Internet access, and electronic messaging systems are referred to collectively as "the
21 computer systems" and are provided in order ~~electronic devices~~, to enhance the educational
22 and business operations of the district. In these regulations, the computers, computer
23 network, electronic devices, Internet access and email system are referred to collectively
24 as "the computer systems."
25

26 These computer systems are business and educational tools. As such, they are ~~being~~ made
27 available to employees of the district for district-related educational and business purposes.
28 *All users of the computer systems must restrict themselves to appropriate district-related*
29 *educational and business purposes.* Incidental personal use of the computer systems may
30 be permitted solely for the purpose of email transmissions and similar communications,
31 including access to the Internet on a limited, occasional basis. Such incidental personal
32 use of the computer systems is subject to all rules, including monitoring of all such use, set
33 out in these regulations. Moreover, any such incidental personal use shall not interfere in
34 any manner with work responsibilities.
35

36 These computer systems are expensive to install, own and maintain. Unfortunately, these
37 computer systems can be misused in a variety of ways, some of which are innocent and
38 others deliberate. Therefore, in order to maximize the benefits of these technologies to the
39 district, our employees and all our students, this regulation shall govern *all* use of these
40 computer systems.
41

42 Monitoring

43
44 It is important for all users of these computer systems to understand that the Board, as the
45 owner of the computer systems, reserves the right to monitor the use of the computer
46 systems to ensure that they are being used in accordance with these regulations. The Board

47 intends to monitor in a limited fashion, but will do so as needed to ensure that the systems
48 are being used appropriately for district-related educational and business purposes and to
49 maximize utilization of the systems for such business and educational purposes. The
50 Superintendent reserves the right to eliminate personal use of the district's computer
51 systems by any or all employees at any time.

52
53 The system administrator and others managing the computer systems may access electronic
54 messaging systems (including email) or monitor activity on the computer system or
55 electronic devices accessing the computer systems at any time and for any reason or no
56 reason. Typical examples include when there is reason to suspect inappropriate conduct or
57 there is a problem with the computer systems needing correction. Further, the system
58 administrator and others managing the computer systems can access or monitor activity on
59 the systems despite the use of passwords by individual users, and can bypass such
60 passwords. In addition, review of emails, messages or information stored on the computer
61 systems, which can be forensically retrieved, includes those messages and/or electronic
62 data sent, posted and/or retrieved using social networking sites, including, but not limited
63 to, Twitter, Facebook, LinkedIn, Instagram and YouTube.

64
65 Notwithstanding the above and in accordance with state law, the Board may not: (1) request
66 or require that an employee provide the Board with a user name and password, password
67 or any other authentication means for accessing a personal online account; (2) request or
68 require that an employee authenticate or access a personal online account in the presence
69 of a Board representative; or (3) require that an employee invite a supervisor employed by
70 the Board or accept an invitation from a supervisor employed by the Board to join a group
71 affiliated with any personal online account of the employee. However, the Board may
72 request or require that an employee provide the Board with a user name and password,
73 password or any other authentication means for accessing (1) any account or service
74 provided by the Board or by virtue of the employee's employment relationship with the
75 Board or that the employee uses for the Board's business purposes, or (2) any electronic
76 communications device supplied or paid for, in whole or in part, by the Board.

77
78 In accordance with applicable law, the Board maintains the right to require an employee to
79 allow the Board to access the employee's personal online account, without disclosing the
80 user name and password, password or other authentication means for accessing such
81 personal online account, for the purpose of:

- 82
- 83 (A) Conducting an investigation for the purpose of ensuring compliance with applicable
84 state or federal laws, regulatory requirements or prohibitions against work-related
85 employee misconduct based on the receipt of specific information about activity on
86 an employee's personal online account; or
 - 87
 - 88 (B) Conducting an investigation based on the receipt of specific information about an
89 employee's unauthorized transfer of the Board's proprietary information,
90 confidential information or financial data to or from a personal online account
91 operated by an employee or other source.
- 92

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

100 Why Monitor?

101
102 The computer systems are expensive for the Board to install, operate and maintain. For
103 that reason alone it is necessary to prevent misuse of the computer systems. However,
104 there are other equally important reasons why the Board intends to monitor the use of these
105 computer systems, reasons that support its efforts to maintain a comfortable and pleasant
106 work environment for all employees.

107
108 These computer systems can be used for improper, and even illegal, purposes. Experience
109 by other operators of such computer systems has shown that they can be used for such
110 wrongful purposes as sexual harassment, intimidation of co-workers, threatening of co-
111 workers, breaches of confidentiality, copyright infringement and the like.

112
113 Monitoring will also allow the Board to continually reassess the utility of the computer
114 systems, and whenever appropriate, make such changes to the computer systems as it
115 deems fit. Thus, the Board monitoring should serve to increase the value of the system to
116 the district on an ongoing basis.

118 Privacy Issues

119
120 Employees must understand that the Board has reserved the right to conduct monitoring of
121 these computer systems and can do so *despite* the assignment to individual employees of
122 passwords for system security. Any password systems implemented by the district are
123 designed solely to provide system security from unauthorized users, not to provide privacy
124 to the individual system user.

125
126 *The system’s security aspects, message delete function and personal passwords can be*
127 *bypassed for monitoring purposes.*

128
129 Therefore, *employees must be aware that they should not have any expectation of personal*
130 *privacy in the use of these computer systems.* This provision applies to any and all uses of
131 the district’s computer systems and electronic devices that access same, including any
132 incidental personal use permitted in accordance with these regulations.

133
134 *Use of the computer system represents an employee’s acknowledgement that the employee*
135 *has read and understands these regulations and any applicable policy in their entirety,*
136 *including the provisions regarding monitoring and review of computer activity.*

140 Prohibited Uses

141
142 Inappropriate use of district computer systems is expressly prohibited, including, but not
143 limited to, the following:

- 144
145 ◆ Sending any form of solicitation not directly related to the business of the Board of
146 Education;
- 147
148 ◆ Sending any form of slanderous, harassing, threatening, or intimidating message,
149 at any time, to any person (such communications *may* also be a *crime*);
- 150
151 ◆ Gaining or seeking to gain unauthorized access to computer systems;
- 152
153 ◆ Downloading or modifying computer software of the district in violation of the
154 district's licensure agreement(s) and/or without authorization from IT Department
155 personnel;
- 156
157 ◆ Damaging equipment through careless handling, loss, or theft;
- 158
159 ◆ Sending any message that breaches the Board's confidentiality requirements,
160 including the confidentiality rights of students;
- 161
162 ◆ Sending any copyrighted material over the system;
- 163
164 ◆ Sending messages for any purpose prohibited by law;
- 165
166 ◆ Storing personal or confidential information on the system;
- 167
168 ◆ Transmission of inappropriate email communications or accessing inappropriate
169 information on the Internet, including vulgar, lewd or obscene words or pictures;
- 170
171 ◆ Using computer systems for any purposes, or in any manner, other than those
172 permitted under these regulations;
- 173
174 ◆ Using social networking sites such as Facebook, Twitter, LinkedIn, Instagram and
175 YouTube in a manner that disrupts or undermines the effective operation of the
176 school district, is used to engage in harassing, defamatory, obscene, abusive,
177 discriminatory or threatening or similarly inappropriate communications; creates a
178 hostile work environment; breaches confidentiality obligations of school district
179 employees, or violates the law, Board policies and/or the other school rules and
180 regulations;
- 181
182 ◆ Violating cybersecurity best practices through the sharing of passwords.
- 183

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

187

188 Electronic Communications

189

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

199

200 Disciplinary Action

201

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

206

207 Complaints of Problems or Misuse

208

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

212

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

218

219 Implementation

220

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

222

223 Legal References:

224

225 Conn. Gen. Stat. § 31-40x

226 Conn. Gen. Stat. § 31-48d

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

228

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

230

#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.

4150 (cont.)

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

**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

33 such students are using Board-owned computers or devices and Board-provided Internet
34 access.

35

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

38

39 Legal References:

40

41 Conn. Gen. Stat. § 10-221

42

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

44

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

47

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

49

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

51

52 Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 U.S.C.
53 § 254(h)(5)(B)(iii)

54

55

56 First Reading: May 9, 2023

57 Second Reading: June 6, 2023

Regulation #5210
Student use of the District’s Computer Systems
and Internet Safety

1
2
3
4
5
6 1. Introduction
7

8 a. Access to District Computer Systems When Students Are Physically Present on School
9 Property
10

11 When students are physically present on school property, the Board is pleased to offer
12 students access to the district's computers and computer networks, including access to
13 electronic messaging systems (including email) and the Internet, as well as electronic
14 devices, (all of which will be referred to collectively as "computer systems"). Access to
15 the school's computer systems will enable students to explore libraries, databases,
16 websites, and bulletin boards while exchanging information with others. Such access is
17 provided solely for education-related purposes. Use of the district's computer systems will
18 be allowed only for students who act in a considerate and responsible manner in using
19 such systems.
20

21 The Board of Education (the “Board”) and the Administration believe in the educational
22 value of such computer systems and recognize their potential to support our curriculum by
23 expanding resources available for staff and student use. The Board’s goal in providing
24 this service is to promote educational excellence by facilitating resource sharing,
25 innovation and communication.
26

27 These computer systems are expensive to purchase, install and maintain. As the property
28 of the district, these computer systems must be carefully handled and their integrity
29 preserved for the benefit of all. Therefore, students are required to adhere to a set of
30 policies and procedures, as set forth in detail below, in conjunction with their use of the
31 computer systems. Violations may lead to withdrawal of the access privilege and/or
32 disciplinary measures in accordance with the Board’s student discipline policy.
33

34 b. Access to District Computer Systems When Students Are Engaged in Remote Learning
35

36 The Board and the Administration recognize that technology is integral to the delivery of
37 instruction if and when the district implements any form of digital or remote learning. The
38 district may therefore provide students with remote access to some or all of the district’s
39 computer systems so that students may access the district’s virtual learning environment.
40 Such access, if granted, is provided solely for education-related purposes. Use of the
41 district's computer systems will be allowed only for students who comply with district
42 policies and procedures concerning computer system use, and demonstrate the ability to
43 use the computer systems in a considerate and responsible manner.
44

45 These computer systems are expensive to purchase, install and maintain. As the property
46 of the district, these computer systems must be carefully handled and their integrity

47 preserved for the benefit of all. Therefore, students will be required to adhere to a set of
48 policies and procedures, as set forth in detail below, in conjunction with their use of the
49 computer systems. Violations may lead to withdrawal of the access privilege and/or
50 disciplinary measures in accordance with the Board’s student discipline policy.

51
52 2. Definitions

53
54 **Obscene** – means any material or performance if, a) taken as a whole, it predominantly
55 appeals to the prurient interest, b) it depicts or describes in a patently offensive way a
56 prohibited sexual act and c) taken as a whole, it lacks serious literary, artistic, educational,
57 political or scientific value.

58
59 **Obscene as to minors - means any material or performance if it depicts a prohibited sexual**
60 **act and, taken as a whole, it is harmful to minors.**

61
62 For purposes of this section, “**harmful to minors**” means that quality of any description or
63 representation, in whatever form, of a prohibited sexual act, when a) it predominantly appeals
64 to the prurient, shameful or morbid interest of minors, b) it is patently offensive to prevailing
65 standards in the adult community as a whole with respect to what is suitable material for
66 minors, and c) taken as a whole, it lacks serious literary, artistic, educational, political or
67 scientific value for minors.

68
69 For the purposes of this section, “**prohibited sexual act**” means erotic fondling, nude
70 performance, sexual excitement, sado-masochistic abuse, masturbation or sexual intercourse.

71
72 **Child pornography** –means any visual depiction, including any photograph, film, video,
73 picture, or computer or computer-generated image or picture, whether made or produced by
74 electronic, mechanical, or other means, of sexually explicit conduct, where -

- 75
76 (a) the production of such visual depiction involves the use of a minor engaging in
77 sexually explicit conduct;
- 78 (b) such visual depiction is a digital image, computer image, or computer-
79 generated image that is, or is indistinguishable from, that of a minor engaging
80 in sexually explicit conduct; or
- 81 (c) such visual depiction has been created, adapted, or modified to appear that an
82 identifiable minor is engaging in sexually explicit conduct.

83
84 3. Monitoring

85
86 Students are responsible for good behavior on school computer systems just as they are in
87 a classroom or a school hallway. Communications on the computer systems are often
88 public in nature and general school rules for behavior and communications apply. It is
89 expected that users will comply with district standards and will act in a responsible and
90 legal manner, at all times in accordance with district standards, as well as with state and
91 federal laws.

93 It is important that students and parents understand that the district, *as the owner of the*
94 *computer systems, reserves the right to monitor and review* the use of these computer
95 systems. The district intends to monitor and review in a limited fashion, but will do so as
96 needed to ensure that the systems are being used for district-related educational purposes.
97

98 As part of the monitoring and reviewing process, the district will retain the capacity to
99 bypass any individual password of a student or other user. *The system's security aspects,*
100 *such as personal passwords and the message delete function for e-mail, can be bypassed*
101 *for these purposes.* The district's ability to monitor and review is not restricted or
102 neutralized by these devices. The monitoring and reviewing process also includes, but is
103 not limited to: oversight of Internet site access, the right to review electronic messages
104 sent and received, the right to track students' access to blogs, electronic bulletin boards
105 and chat rooms, and the right to review a student's data downloading and printing.
106

107 Therefore, all users must be aware that *they should not have any expectation of personal*
108 *privacy in the use of these computer systems.*
109

110 4. Student Conduct

111
112 Students are permitted to use the district's computer systems for legitimate educational
113 purposes. Personal use of district computer systems is expressly prohibited. Conduct which
114 constitutes inappropriate use includes, but is not limited to the following:
115

- 116 ♦ Sending any form of a harassing, threatening, or intimidating message, at any time, to
117 any person (such communications may also be a crime);
- 118
- 119 ♦ Gaining or seeking to gain unauthorized access to computer systems;
- 120
- 121 ♦ Damaging computers, computer files, computer systems or computer networks;
- 122
- 123 ♦ Downloading or modifying computer software of the district in violation of the
124 district's licensure agreement(s) and/or without authorization from a teacher or
125 administrator;
- 126
- 127 ♦ Using another person's password under any circumstances;
- 128
- 129 ♦ Trespassing in or tampering with any other person's folders, work or files;
- 130
- 131 ♦ Sending any message that breaches the district's confidentiality requirements, or the
132 confidentiality of students;
- 133
- 134 ♦ Sending any copyrighted material over the system;
- 135
- 136 ♦ Using computer systems for any personal purpose or gain, or in a manner that
137 interferes with the district's educational programs;
- 138

- 139 ♦ Accessing or attempting to access any material that is obscene, obscene as to minors,
140 or contains child pornography, as defined above;
- 141
- 142 ♦ Transmitting e-mail communications or accessing information on the Internet for non-
143 educational purposes;
- 144
- 145 ♦ Cyberbullying;
- 146
- 147 ♦ Accessing or attempting to access social networking sites (e.g., Facebook, Twitter,
148 Instagram, Snapchat, TikTok, etc.) without a legitimate educational purpose.
- 149

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

153
154 *Misuse of the computer systems, or violations of these policies and regulations, may result in*
155 *loss of access to such computer systems as well as other disciplinary action, including*
156 *suspension and/or expulsion, depending on the specific conduct.*

157
158 Anyone who is aware of problems with, or misuse of, these computer systems, or has a
159 question regarding the proper use of these computer systems, should report or discuss the
160 issue with a teacher or the school principal immediately. Most importantly, the Board and the
161 Administration urge *any* student who receives *any* harassing, threatening, intimidating or
162 other improper message through the computer system to report this immediately. It is the
163 Board's policy that no student should be required to tolerate such treatment, regardless of the
164 identity of the sender of the message. *Please report these events!*

165
166 5. Internet Safety

167
168 The Administration will take measures: to assure the digital safety and security of students
169 when using electronic messaging systems, email, chat rooms, distance learning platforms, and
170 other forms of direct electronic communications; to prohibit unauthorized access, including
171 “hacking” and other unlawful activities by minors online; to prohibit unauthorized disclosure,
172 use, and dissemination of personally identifiable information regarding students; to educate
173 minor students about appropriate online behavior, including interacting with other individuals
174 on social networking websites and in chat rooms and cyber-bullying awareness and response;
175 and to restrict students’ access to online materials that are obscene or obscene as to minors or
176 contain child pornography, to the extent practicable when students are using Board-owned
177 computers or devices and Board-provided Internet access.

178
179 6. Student Use Agreement

180
181 Before being allowed to use the district’s computer systems, students and/or their
182 parents/guardians must sign a computer system use agreement, stating that they have read and
183 understood the district’s policies and regulations regarding the use of its computer systems.

184
185 Legal References:

186
187 Conn. Gen. Stat. § 10-221
188
189 Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250 *et. seq.* (computer-related offenses)
190
191 Conn. Gen. Stat. § 53a-193 (definition of obscene and obscene as to minors)
192
193 18 U.S.C. § 2256 (definition of child pornography)
194
195 Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 18
196 U.S.C. §§ 2510 through 2520
197
198 Children’s Internet Protection Act, Pub. Law 106-554, codified at 47 U.S.C. § 254(h)
199
200 No Child Left Behind Act of 2001, Pub. L. 107-110, codified at 20 U.S.C. § 6777
201
202 Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 U.S.C.
203 § 254(h)(5)(B)(iii)
204
205 Miller v. California, 413 U.S. 15 (1973) (definition of obscene)
206
207
208
209
210

#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, iPads or other tablet computers, walkie talkies, Blackberries, personal data assistants, iPhones, Androids and other electronic signaling devices.

#5090.9(b)

34
35 **Use of Privately-Owned Technological Devices**
36

37 Privately-owned technological devices may not be used during instructional time, except
38 as specifically permitted by instructional staff or unless necessary for a student to access
39 the district’s digital learning platform or otherwise engage in remote learning [if remote](#)
40 [learning has been authorized in accordance with applicable law](#).
41

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

- 47
- 48 • Sending any form of a harassing, threatening, or intimidating message, at any
49 time, to any person (such communications may also be a crime);
50
- 51 • Gaining or seeking to gain unauthorized access to Board technology resources;
52
- 53 • Damaging Board technology resources;
54
- 55 • Accessing or attempting to access any material that is obscene, obscene as to
56 minors, or contains pornography;
57
- 58 • Cyberbullying;
59
- 60 • Using such device to violate any school rule, including the unauthorized
61 recording (photographic, video, or audio) of another individual without the
62 permission of the individual or a school staff member; or
63
- 64 • Taking any action prohibited by any Federal or State law.
65
66

67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97

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-

98

#5090.9(d)

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

101

102

103 **Access to Board Technology Resources**

104

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

115

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

119

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

127

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

131 school accounts. No user may deviate from these log-on/access procedures. **Students**
132 **are advised that the Board’s network administrators have the capability to identify**
133 **#5090.9(e)**
134 **users and to monitor all privately-owned technological devices while they are logged**
135 **on to the network.** Students must understand that the Board has reserved the right to
136 conduct monitoring of Board technology resources and can do so *despite* the assignment
137 to individual users of passwords for system security. Any password systems implemented
138 by the Board are designed solely to provide system security from unauthorized users, not
139 to provide privacy to the individual system user. The system's security aspects, message
140 delete function and personal passwords can be bypassed for monitoring purposes.
141 Therefore, students should be aware that they should not have any expectation of personal
142 privacy in the use of privately-owned technological devices to access Board technology
143 resources. This provision applies to any and all uses of the Board’s technology resources
144 and any privately-owned technological devices that access the same.

145

146 **Harm to Board Technology Resources**

147

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

152

153 **Closed Forum**

154

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

156

157 Legal References:

158

159 Conn. Gen. Stat. § 10-233j

160

161 Conn. Gen. Stat. § 31-48d

162

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

164

165 Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at
166 28 U.S.C. §§ 2510 through 2520

167

168

169 Date of Adoption: September 5, 1995

170 Date of Revision: October 15, 1996

171 Date of Revision: December 1, 1998

172 Date of Revision: April 23, 2002

173 Date of Revision: June 1, 2010

174 Date of Revision: June 5, 2012

175 Date of Revision: October 15, 2013

176 Date of Revision: June 21, 2022

177

178 First Reading: May 9, 2023

179 Second Reading: June 6, 2023