



HARTLAND CONSOLIDATED SCHOOLS

Draft - Policy Manual

10-12-26 Policy Committee Sept update

18 policies

October 9, 2026

Table of Contents

01 - OVERVIEW Vol.41, No. 1 - September 2026

po0100	DEFINITIONS Revised
po0154	MOTIONS Revised
po0164.1	MEETINGS Revised
po0164.2	SPECIAL MEETINGS Rescind
po0165.1	REGULAR MEETINGS Rescind
po0165.2	CHANGE OF REGULAR MEETINGS Rescind
po0165.4	EMERGENCY MEETINGS Rescind
po0165.5	RECESS Rescind
po0165.6	CANCELLATION Rescind
po3310	FREEDOM OF SPEECH IN NON-OFFICIAL DUTY SETTINGS Revised
po4310	FREEDOM OF SPEECH IN NON-OFFICIAL DUTY SETTINGS Revised
po5330.01	EPINEPHRINE DELIVERY SYSTEMS Revised
po7540.03	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY Revised
po7540.04	STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY Revised
po8310	PUBLIC RECORDS Revised
po8321	CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY) Revised
po8420	EMERGENCY SITUATIONS AT SCHOOLS Revised



10-12-26 POLICY COMMITTEE SEPT UPDATE

01 - OVERVIEW

Vol.41, No. 1 - September 2026

MICHIGAN LOCAL UPDATE OVERVIEW AND COMMENTS

VOLUME 41 NUMBER 1

SEPTEMBER 2026

BYLAWS AND POLICIES

Bylaw 0100 - Definitions (Revised)

Bylaw 0100 - Definitions is important because it establishes clear, legally aligned definitions for the terms used throughout all District policies and bylaws.

This revision includes the new term School Support Organizations (SSOs). It is recommended that this revision be adopted as policies and guidelines in this update, and future updates will use this terminology.

Bylaw 0154 - Organizational Meeting Actions (Replacement)

This policy outlines the specific legal and operational mandates required during the school board's annual organizational meeting, ensuring the board stays fully compliant with state law from day one. By standardizing essential actions—such as electing officers, setting regular meeting schedules, and designating official depositories—it establishes clear leadership roles and fiscal governance for the entire upcoming year. Additionally, it provides flexibility by allowing the board to designate key administrative roles and committee structures, setting a solid foundation for efficient, transparent district operations.

The revisions include a new policy title, requirements within the organizational meeting, as well as options that can take place at the organizational meeting or a future meeting. It is recommended that the revisions to this policy be adopted.

Policy 0164.1 - Meetings (Revised)

Policy 0164.1 has been revised by including updated content from eight (8) related policies, all of which are being rescinded in this update. The goal of this consolidation is to create one (1) policy that governs the related statutory requirements.

This consolidated policy governs how regular, special, emergency, and recessed board meetings are scheduled, noticed, and conducted in accordance with the Open Meetings Act. It ensures strict legal compliance and public transparency by establishing precise timelines and required locations—both physical and digital—for posting meeting notices. Additionally, it safeguards board operations by defining narrow legal exceptions for electronic participation and providing clear protocols to handle emergency sessions safely and lawfully.

The revisions to this policy and the rescinded policy delineated below are highly recommended.

The Policies to be rescinded in this update and as described above in Policy 0164.1 - Meetings include:

- **Policy 0164.2 - Special Meetings (Rescinded)**
- **Policy 0164.3 - Emergency Meetings (Rescinded)**
- **Policy 0165.1 - Regular Meetings (Rescinded)**
- **Policy 0165.2 - Change of Regular Meetings (Rescinded)**
- **Policy 0165.4 - Emergency Meetings (Rescinded)**
- **Policy 0165.5 - Recess (Rescinded)**
- **Policy 0165.6 - Cancellation (Rescinded)**

Rescinding all of these policies is highly recommended, as their updated content is reflected in the consolidation/revision/update of Policy 0164.1 - Meetings.

Policy 3310/4310 - Freedom of Speech in Non-Official Duty Settings (Revised)

These policies establish clear boundaries to protect employees' First Amendment rights while safeguarding the school district from potential operational disruptions. It clarifies that staff members speak as private citizens—not on behalf of the district—when expressing personal views outside their official duties.

These policy revisions establish clear boundaries when expressing personal views outside their official duties. By outlining expectations against disruptive, threatening, or privacy-invading speech across all platforms, including social media, the language protects the district from legal liability while safeguarding employees' First Amendment and statutory rights through fair, neutral, case-by-case enforcement.

These revisions are highly recommended as they provide the District and all staff with updated guidance relative to protected speech and related issues.

Policy 5330 - Use of Medications (Revised)

This policy ensures student health and safety by establishing clear protocols for administering both prescribed and over-the-counter medications at school while maximizing the district's statutory liability protection under Michigan law. It also gives

families appropriate flexibility for emergency medications like inhalers and epinephrine so students can safely manage chronic conditions while attending school.

While allowing over-the-counter ("OTC") medications with only parent consent is more convenient for families, requiring a physician's order for **all** medications gives the district the strongest legal shield and statutory immunity protection under state law. Additionally, it protects school nurses and staff from practice-act violations, ensuring they never administer nonprescription drugs without the formal medical orders their professional licenses require. Districts should carefully consider the recommended policy revisions.

This policy was recently revised by the District Nurse to include these recommendations, so there are no changes at this time.

Policy 5330.01 - Epinephrine Delivery Systems (Revised)

This policy ensures schools are legally compliant and prepared to quickly handle life-threatening allergic reactions by allowing trained staff to administer emergency epinephrine, regardless of whether a student has a pre-existing prescription on file. Updating the language to "epinephrine delivery systems" broadens protection beyond standard auto-injectors (like Epi-Pens) to include newer FDA-approved methods such as nasal sprays and inhalers.

The policy revisions align with Michigan statutory updates which transitioned the terminology from narrower "epinephrine auto-injectors" (Epi-Pens) to the comprehensive term "**epinephrine delivery systems**". This encompasses newly FDA-approved administration methods such as epinephrine nasal sprays and inhalers alongside traditional auto-injectors.

The policy revisions are recommended as they align with Michigan code.

Policy 7540.03 - Student Technology Acceptable Use and Safety (Revised)

This policy is important because it guides students' online safety and also provides guidance on the use of school computers and the internet.

The updates are important because they introduce new rules regarding information generated by Artificial Intelligence (AI) tools. Any student who misuses AI in these harmful ways may be subject to discipline, up to and including expulsion, and shall be reported to law enforcement.

These changes are recommended.

Policy 7540.04 - Staff Technology Acceptable Use and Safety (Revised)

This policy is important because it sets clear safety rules for how school staff can use the internet and District technology.

The updates are important because they create new information for using Artificial Intelligence ("AI") tools at work. These changes protect the school community by banning staff from entering private student data into AI systems and strictly prohibiting the creation of fake or inappropriate images. Staff members who violate the provisions of this policy may be subject to discipline, up to and including termination, and reporting to law enforcement.

These changes are recommended.

Policy 8310 - Public Records (Revised)

This policy requires the District to safely maintain its official records and make them available for public inspection or copying.

The updates clarify that any communications or files created by Artificial Intelligence ("AI"), social media, or personal devices are also public records subject to these rules. In addition, the changes indicate that large or complex requests may take longer to complete.

These changes are recommended.

Policy 8321 - Criminal Justice Information Security (Non-Criminal Justice Agency) (Revised)

Policy 8321 is important because it establishes strict security, access, and confidentiality standards for handling criminal history record information obtained through state and federal background checks. Adhering to these requirements ensures school district compliance with Michigan State Police and FBI regulations while safeguarding sensitive employee and applicant data from unauthorized exposure.

Based on feedback from the Michigan Police Association, we have revised the policy to reflect future audit preparations.

The policy revisions are recommended for adoption.

Policy 8420 - Emergency Situations at Schools (Revised)

This policy is important because it establishes clear, standardized emergency requirements so students and staff can react quickly and safely during a crisis like a fire, severe weather, or security threat. It also provides direction so that schools stay prepared and accountable by requiring regular safety drills and public posting of their completion results.

The revisions include the requirement that all schools use consistent terms and definitions for emergency responses. These terms include: Hold, Secure, Lockdown, Evacuate, and Shelter. Aligning these terms across all training, drills, and official plans builds clear expectations and legal compliance, allowing for a faster, more coordinated response when safety is at risk.

The Cardiac Emergency Response Plan section has also been revised to provide statutory alignment and clarity.

These revisions are required to align with statutes.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0100

DEFINITIONS Revised

ADOPTED Jan 28, 2008 · REVISED Apr 20, 2026

0100 - DEFINITIONS

The bylaws of the Board of Education of this District incorporate quotations from the laws and administrative code of the State of Michigan. Such quotations may be substantively altered only by appropriate legislative, judicial, or administrative action.

Whenever the following items are used in these bylaws and policies, they shall have the meaning set forth below:

Administrative Guideline

A statement, based on policy, usually written, which outlines and/or describes the means by which a policy should be implemented and which provides for the management cycle of planning, action, and assessment or evaluation.

Agreement

A collectively negotiated contract with a recognized bargaining unit.

Apps and Services

Apps and services are software (i.e., computer programs) that support the interaction of personal communication devices (as defined in Bylaw 0100) over a network, or client-server applications in which the user interface runs in a web browser. Apps and services are used to communicate/transfer information/data that allow students to perform actions/tasks that assist them in attaining educational achievement goals/objectives, enable staff to monitor and assess their students' progress, and allow staff to perform other tasks related to their employment. Apps and services also are used to facilitate communication to, from and among and between, staff, students, and parents, Board members and/or other stakeholders and members of the community.

Board

The Board of Education.

Bylaw

Rule of the Board for its own governance.

Classified or Support Employee

An employee who provides support to the District's program and whose position does not require a professional certificate.

District

The School District.

Due Process

Procedural due process requires prior knowledge (a posted discipline code), notice of offense (accusation), and the opportunity to respond.

Procedural due process may require consideration of statutorily mandated factors, right to counsel and/or confrontation or cross-examination of witnesses, depending upon the situation.

Family Member

"Family member" means a person's spouse or spouse's sibling or child; a person's sibling or sibling's spouse or child; a person's child or child's spouse; or a person's parent or parent's spouse, and includes these relationships as created by adoption or marriage. (See Bylaw 0144.3)

Full Board

Authorized number of voting members entitled to govern the District.

Information Resources

The Board defines Information Resources to include any data/information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of data/information. This definition includes but is not limited to electronic mail, voice mail, social media, text messages, databases, CD-ROMs/DVDs, websites, motion picture film, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any equipment, computer facilities, or online services used in accessing, storing, transmitting or retrieving electronic communications.

May

This word is used when an action by the Board or its designee is permitted but not required.

Meeting

Any gathering which is attended by or open to all of the members of the Board held with the intent on the part of the members of the body present to discuss or act as a unit upon the specific public business of that body.

Parent

The natural or adoptive parents, or individuals with a valid power of attorney for the care and custody of the student for purposes other than educational placement. Parent refers to any individual appointed by the State or court as a legal guardian or custodian for the student. Both parents will have equal access to records and rights regarding the student's education absent a court order restricting such rights.

Personal Communication Devices

Personal communication devices ("PCDs") may include computers, laptops, tablets, e-readers, wireless communication devices ("WCDs"), cellular/mobile phones, smartphones, and/or other web-enabled devices of any type.

Policy

A general, written statement by the governing Board which defines its expectations or position on a particular matter and authorizes appropriate action that must or may be taken to establish and/or maintain those expectations.

President

The chief executive officer of the Board of Education. (See Bylaw 0171.1)

Principal

The educational leader and head administrator of one (1) or more District schools or programs, as designated by the Board of Education. The Principal must hold an appropriate school administrator certificate or permit. The Principal is responsible for the supervision of the school or program consistent with Board policy and directives of the Superintendent and may delegate responsibility to subordinates as appropriate.

Professional Staff Member

An employee who implements or supervises one (1) or more aspects of the District's program and whose position requires a professional credential from the State.

Relative

The mother, father, sister, brother, spouse, parent of spouse, child, grandparents, grandchild, or dependent in the immediate household as defined in the negotiated, collectively-bargained agreement.

School Support Organizations (SSOs)

Any other nongovernmental organization or group of persons whose primary purpose is to support a District, school, school club, or academic, arts, athletic, or social activities related to a school, that collects or receives money, materials, property, or securities from students, parents, or members of the general public. (Examples: Booster Club, Foundation, Parent-Teacher Association (PTA), Parent-Teacher Organization (PTO), Parent-Teacher Support Association)

Secretary

The chief clerk of the Board of Education. (See Bylaw 0171.3)

Shall

This word is used when an action by the Board or its designee is required. (The word "will" or "must" also signifies a required action.)

Social Media

Social media are online platforms where users engage one another and/or share information and ideas through text, video, or pictures. Social media consists of any form of online publication or presence that allows interactive communication, including, but not limited to, text messaging, instant messaging, websites, web logs ("blogs"), wikis, online forums (e.g., chat rooms), virtual worlds, and social networks. Examples of social media include, but are not limited to, Facebook, Facebook Messenger, Google Hangouts, X (f.k.a. Twitter), LinkedIn, YouTube, Flickr, Instagram, Pinterest, Skype, and Facetime. Social media does not include sending or receiving e-mail through the use of District-issued e-mail accounts.

Student

A person who is officially enrolled in a school or program of the District.

Superintendent

The chief executive officer of the School District is responsible to supervise all programs and staff of the District and to implement Board policy and follow Board directives. The Superintendent must hold an appropriate school administrator certificate or permit. Consistent with Board policies and directives. The Superintendent may delegate responsibility to subordinates as appropriate.

Technology Resources

The Board defines Technology Resources to include computers, laptops, tablets, e-readers, cellular/mobile telephones, smartphones, web-enabled devices, video and/or audio recording equipment, projectors, software and operating systems that work on any device, copy machines, printers and scanners, information storage devices (including mobile/portable storage devices such as external hard drives, CDs/DVDs, USB thumb drives and memory chips), the computer network, Internet connection, and online educational services and apps.

Treasurer

The chief financial officer of the District. (See Bylaw 0171.4)

Vice-President

The Vice-President of the Board of Education. (See Bylaw 0171.2)

Voting

A vote at a meeting of the Board of Education. Except to accommodate the absence of any member of the Board due to military duty, or for any other purpose permitted by law, Board members must be physically present in order to have their vote officially recorded in the Board minutes.

Wireless Communication Device ("WCD")

For the purposes of Policy/Administrative Guideline 5136 - Wireless Communication Devices (WCDs), a WCD is an electronic device capable of, but not limited to, text messaging, voice communication, entertainment, navigation, accessing the internet, sending and receiving photos and videos, or producing email. A WCD does not include a basic telephone, which is a device primarily used for voice calling that cannot support third-party applications, except those preinstalled, and does not support access to internet platforms via applications or web browsers.

Citations to Michigan Compiled Laws (M.C.L.) are shown as M.C.L. followed by the Section Number (e.g., M.C.L. 380.1438). Citations to the Michigan Administrative Code are prefaced A.C. Rule (e.g., A.C. Rule R380.221). Citations to the Federal Register are noted as F.R., to the Code of Federal Regulations as C.F.R., and to the United States Code as U.S.C.

Revised 12/17/18
Revised 6/10/19
Revised 12/15/21

© Neola 2026

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0154

MOTIONS Revised

ADOPTED Jan 28, 2008

0154 - ORGANIZATIONAL MEETING ACTIONS **MOTIONS**

[DRAFTING NOTE: Michigan Law requires only two (2) specific actions that must occur at the annual organizational meeting. Those actions include the election of officers and establishing the time and place of regular meeting locations. Additional options have been provided.]

The Board shall, at the organizational meeting, take the following actions, including but not limited to:

- A. designate depositories for school funds; M.C.L.A. 380.1221
- B. designate those persons authorized to sign checks, contracts, agreements, and purchase orders;
- C. designate a day, place, and time for regular meetings which shall be held at least once every month;
- D. designate an administrator to assume specified duties **responsibilities** of the Treasurer or **and of the** Secretary, consistent with law;
- E. designate the Electronic Transfer Officer (ETO) in accordance with Policy 6144.

[x] Election of Officers - President, Vice President, Secretary, and Treasurer;

[x] Designation of legal counsel and auditor;

[.] Designation of a FOIA Coordinator;

[.] Adoption of parliamentary authority;

[.] Establishment of committees;

[x] other organizational matters as deemed appropriate by the Board

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0164.1

MEETINGS Revised

ADOPTED Jan 28, 2008

0164.1 - **REGULAR** MEETINGS

Regular Meetings

The Board shall hold a meeting at least once each month on a date and at a time and place determined annually by a resolution of the Board.

Posting of Regular Board Meetings

Within ten (10) days after the organizational Board meeting, the Board shall post at the Board office and in other locations considered appropriate by the Board, a notice listing the date, time, and place of each regularly scheduled meeting of the Board. If the District maintains an official website, the notice shall also be posted on a dedicated public-notice webpage on the District's website, or through a prominent and conspicuous link to that webpage on the District's homepage. The notice shall contain the name and address of the District and its telephone number.

The notice shall also contain the following statement:

"Upon request to the Superintendent, the District shall make reasonable accommodation for a person with disabilities to be able to participate in this meeting."

Upon the written request of an individual, organization, firm, or corporation, and upon the requesting party's payment of a yearly fee of not more than the actual reasonable cost for printing and postage of each notice, the District shall send to the requesting party by first-class mail a copy of any notice required to be posted by the Open Meetings Act.

Public information bodies and the news media shall be entitled to receive these notices without charge.

Change in Schedule

If the Board decides to change its regular meeting schedule (e.g., moving a standing Tuesday meeting to a Wednesday), a new notice must be posted within three (3) days after

the meeting where the change was made. This requirement also applies to dates, times, or places of previously scheduled meetings.

Special Meetings

Special meetings of the Board may be called by the President or by any two (2) members of the Board provided there is compliance with the notice provision of these Bylaws.

The notice for any special meeting shall include the date, time, and place of the meeting, the business to be transacted, and the name, address, and telephone number of the District.

In accordance with the Open Meetings Act:

A. Physical Posting: The notice shall be posted at the District's principal office and any other locations designated by the Board at least eighteen (18) hours prior to the meeting.

B. Digital Posting: If the District maintains an official website, the notice must also be posted on a public-notice webpage (or a prominent link) on that website for at least eighteen (18) hours before the meeting begins.

C. Board Notification: A copy of the notice shall be provided to each member of the Board

Emergency Meetings

A Board may meet in an emergency session without the eighteen (18) hour notice only if there is a severe and imminent threat to the health, safety, or welfare of the public, and two-thirds (2/3s) of the members agree that a delay would be detrimental. This must be a roll call vote.

A. Military Duty: A Board member may participate and vote remotely if their absence is due to active military duty.

B. ADA Accommodation: As a reasonable accommodation under the Americans with Disabilities Act (ADA), a Board member with a qualified disability may be permitted to participate and vote remotely.

Meeting Recess

Any meeting of the Board may be recessed to another time and place. Any meeting which is recessed for more than thirty-six (36) hours shall be reconvened only after a notice stating the date, time, and place of the recessed meeting, as well as the name, address, and telephone number of the District has been posted on the front door of the Administrative Office Building , and on a prominent and conspicuous portion of the District's

website, and such other place(s) as the Board may determine for at least eighteen (18) hours prior to the time the meeting is to be reconvened.

If the recessed meeting will involve remote participation by a Board member as expressly authorized by the Open Meetings Act or other applicable law, the notice must also include information on how the public may participate or contact the remote member.

Meeting Cancellation

Any meeting of the Board may be cancelled for appropriate purposes, which shall include, but not be limited to, inclement weather, lack of a quorum, or conflict with a special event relating to the District. If the cancelled meeting is a regular meeting, it must be rescheduled, following all notice requirements set forth above.

Disclosure Requirements

Any Board member participating remotely must, at the beginning of the meeting, announce for the record that they are attending remotely. Unless the absence is due to military duty, the member must specifically state the physical location (City/Township and State) from which they are attending. This information shall be included in the meeting minutes.

Public Attendance and Participation

The Board may, at its discretion, provide a digital platform for the public to observe and/or participate in meetings.

A. Two-Way Communication: If a meeting is held with remote participation options, the platform used must allow for two-way communication so that the public may hear the Board and the Board may hear public comments.

B. Notice Requirements: Digital notices for meetings with a remote component must be posted on the District's website homepage (or a conspicuous link therefrom) and must include instructions on how the public may participate and contact Board members to provide input.

© Neola ~~2017~~ 2026

Legal

M.C.L. 15.251

M.C.L. 15.263

M.C.L. 15.264

M.C.L. 15.265



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0164.2

SPECIAL MEETINGS Rescind

ADOPTED Jan 28, 2008 · REVISED Apr 20, 2026

0164.2 - SPECIAL MEETINGS

Special meetings of the Board may be called by the President or two (2) members of the Board provided there is compliance with the notice provision of these Bylaws.

Said notice shall state the date, time, and place of such special meeting and the business to be transacted thereat, as well as the name, address, and telephone number of the District.

A notice of any special meeting shall be posted at least eighteen (18) hours before said special meeting at the Board office and such other places as the Board may determine. A copy of said notice shall be served upon each member of the Board.

Revised 1/9/23

Revised 12/16/24

© Neola 1996



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0165.1

REGULAR MEETINGS Rescind

ADOPTED Jan 28, 2008

0165.1- **REGULAR MEETINGS**

Within ten (10) days after the organizational Board meeting, the Board shall cause to be posted at the Board office and in other locations considered appropriate by the Board, a notice listing the date, time, and place of each regularly scheduled meeting of the Board. The notice shall contain the name and address of the District and its telephone number. The notice shall also contain the following statement:

"Upon request to the Superintendent, the District shall make reasonable accommodation for a person with disabilities to be able to participate in this meeting."

Upon the written request of an individual, organization, firm, or corporation, and upon the requesting party's payment of a yearly fee of not more than the estimated reasonable cost for printing and postage of each notice as shall be determined annually by the Board, the District shall send to the requesting party by first-class mail a copy of any notice required to be posted by these bylaws. The news media shall be entitled to receive, at their request, copies of such notices free of charge.

© Neola 2017



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0165.2

CHANGE OF REGULAR MEETINGS Rescind

ADOPTED Jan 28, 2008

0165.2 - **CHANGE OF REGULAR MEETINGS**

Within three (3) days after the Board adopts a resolution changing the date, time, or place of a regularly scheduled meeting, the meeting notice shall state the date, time, and place of the rescheduled meeting, as well as the name, address, and telephone number of the District. Said notice shall be posted on the front door of the Administrative Office Building and such other place(s) as the Board may determine. Said notice shall be posted at least eighteen (18) hours before the rescheduled meeting.

© Neola 2017

Legal

M.C.L.A. 15.264, 15.266



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0165.4

EMERGENCY MEETINGS Rescind

ADOPTED Jan 28, 2008

~~0165.4 - EMERGENCY MEETINGS~~

~~No notice of any emergency meeting shall be required.~~

~~© Neola 2017~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0165.5

RECESS Rescind

ADOPTED Jan 28, 2008

0165.5 - RECESS

Any meeting of the Board may be recessed to another time and place. Any meeting which is recessed for more than thirty-six (36) hours shall be reconvened only after a notice stating the date, time, and place of the recessed meeting as well as the name, address, and telephone number of the District has been posted on the front door of the Administrative Office Building and such other place as the Board may determine for at least eighteen (18) hours prior to the time the meeting is to be reconvened.

© Neola 2017

Legal

M.C.L.A. 15.265, 380.1201(3)(4)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po0165.6

CANCELLATION Rescind

ADOPTED Dec 17, 2018

0165.6 -- **CANCELLATION**

Any meeting of the Board may be canceled for appropriate purposes, which shall include, but not be limited to, inclement weather, lack of a quorum, or conflict with a special event relating to the District. If the canceled meeting is a regular meeting it must be re-scheduled following all notice requirements set forth above.

© Neola 2018

Legal

M.C.L. 15.265, 380.1201(3)(4)



10-12-26 POLICY COMMITTEE SEPT UPDATE

po3310

FREEDOM OF SPEECH IN NON-OFFICIAL DUTY SETTINGS Revised

ADOPTED Jan 28, 2008

3310 - FREEDOM OF SPEECH IN **NON-OFFICIAL DUTY** **NONINSTRUCTIONAL** SETTINGS

This policy applies to professional staff members' speech outside the scope of their official duties as employees of the District (i.e., outside the classroom, school-sponsored events, or similar). The Board of Education acknowledges the right of its professional staff members, as citizens in a democratic society, to speak out on issues of public concern. When those issues are related to the District, however, the professional staff member's expression must be balanced against the interests of this District. For example, such expression must not be disruptive to the District and/or the staff member's ability to perform their job. Similarly, a staff member's opinions or views are not those of the District and may not be represented as such, regardless of the forum. These determinations will be made in the District's discretion.

The following guidelines are adopted by the Board to help clarify and, therefore, avoid situations in which the professional staff member's expression could conflict with the District's interests. In such situations, **s/he** the staff member should:

- A. state clearly that their **his/her** expression represents personal views and not necessarily those of the School District;
- B. refrain from expressions that would invade the rights of others, create disruption within the District, **disrupt harmony among co-workers** or interfere with the maintenance of discipline by school officials;
- C. not make threats , disrespectful, -or abusive , or **personally-**defamatory comments about students or their family members, co-workers, administrators, or officials of the District , or other individuals or entities which may have a relationship with the District;
- D. refrain from making public expressions which the staff member **s/he** knows to be false or are made without regard for truth or accuracy.

Nothing in this policy is intended to limit the District's ability to make disciplinary or termination decisions in accordance with applicable law regarding any unprotected expression, and this policy should be treated as guidance and not a full itemization of potentially unprotected expression. Nor should this policy be treated as defining the full protected rights of staff members; the District will apply this policy on a case-by-case basis in accordance with the applicable law. Furthermore, this policy applies to all forums of expression including, but not limited to, written form (digital, print, etc.), verbal, physical, visual, via social media (such as X, Facebook, Instagram, LinkedIn, blogs, websites, etc.), and via other electronic communications (email, messaging, etc.). It also applies regardless of the manner of speech, whether written, visual, digital, verbal, graphic, or otherwise. Note that conduct that violates the District's policies including, but not limited to, those addressing discrimination and/or harassment policies, may result in disciplinary action, even if such conduct does not specifically violate this policy.

Employees who engage in constitutionally protected speech will not be retaliated against, and this policy will be applied equally, regardless of the viewpoint expressed. Nothing in this policy is intended to, or will be enforced to, limit an employee's right to engage in activities that are protected by applicable law including, but not limited to, rights protected by the Public Employer Relations Act, the right to engage in protected whistleblower activity, or similarly protected activities. **This policy in no way impacts the obligations of an employee who is a mandatory reporter by State law.**

© Neola 2026



10-12-26 POLICY COMMITTEE SEPT UPDATE

po4310

FREEDOM OF SPEECH IN NON-OFFICIAL DUTY SETTINGS Revised

ADOPTED Jan 28, 2008

4310 - FREEDOM OF SPEECH IN **NON-OFFICIAL DUTY** **NONINSTRUCTIONAL** SETTINGS

This policy applies to support staff members' speech outside the scope of their official duties as employees of the District (i.e., outside the classroom, school-sponsored events, or similar). The Board of Education acknowledges the right of its support staff members, as citizens in a democratic society, to speak out on issues of public concern. When those issues are related to the District, however, the support staff member's expression must be balanced against the interests of this District. For example, such expression must not be disruptive to the District and/or the staff member's ability to perform their job. Similarly, a staff member's opinions or views are not those of the District and may not be represented as such, regardless of the forum. These determinations will be made in the District's discretion.

The following guidelines are adopted by the Board to help clarify and, therefore, avoid situations in which the support staff member's expression could conflict with the District's interests. In such situations, the staff member **s/he** should:

- A. state clearly that their **his/her** expression represents personal views and not necessarily those of the School District;
- B. refrain from expressions that would invade the rights of others, create disruption within the District, **disrupt harmony among co-workers** or interfere with the maintenance of discipline by school officials;
- C. not make threats , disrespectful, or abusive , or **personally** defamatory comments about students or their family members, co-workers, administrators, or officials of the District , or other individuals or entities which may have a relationship with the District;
- D. refrain from making public expressions which the staff member **s/he** knows to be false or are made without regard for truth or accuracy.

Nothing in this policy is intended to limit the District's ability to make disciplinary or termination decisions in accordance with applicable law regarding any unprotected expression, and this policy should be treated as guidance and not a full itemization of potentially unprotected expression. Nor should this policy be treated as defining the full protected rights of staff members; the District will apply this policy on a case-by-case basis in accordance with the applicable law. Furthermore, this policy applies to all forums of expression including, but not limited to, written form (digital, print, etc.), verbal, physical, visual, via social media (such as X, Facebook, Instagram, LinkedIn, blogs, websites, etc.), and via other electronic communications (email, messaging, etc.). It also applies regardless of the manner of speech, whether written, visual, digital, verbal, graphic, or otherwise. Note that conduct that violates the District's policies including, but not limited to, those addressing discrimination and/or harassment policies, may result in disciplinary action, even if such conduct does not specifically violate this policy.

Employees who engage in constitutionally protected speech will not be retaliated against, and this policy will be applied equally regardless of the viewpoint expressed. Nothing in this policy is intended to, or will be enforced to, limit an employee's right to engage in activities that are protected by applicable law including, but not limited to, rights protected by the Public Employer Relations Act, the right to engage in protected whistleblower activity, or similarly protected activities. **This policy in no way impacts the obligations of an employee who is a mandatory reporter by State law.**

10-12-26 POLICY COMMITTEE SEPT UPDATE

po5330.01

EPINEPHRINE DELIVERY SYSTEMS Revised

ADOPTED Jun 9, 2014 · REVISED Sep 15, 2025

5330.01 - EPINEPHRINE DELIVERY SYSTEMS AUTO-INJECTORS

Students who are prescribed epinephrine to treat anaphylaxis shall be allowed to self-possess and self-administer the medication if they meet the conditions as stated in Policy 5330.

[DRAFTING NOTE: "Epinephrine delivery system" means a device containing a premeasured dose of epinephrine that is used for the treatment of anaphylaxis. This includes, but is not limited to, epinephrine auto-injectors (such as Epi-Pens), epinephrine inhalers, and epinephrine nasal sprays. For the purposes of this policy, any reference to "injection" or "administration" shall encompass the use of any such delivery system in accordance with the manufacturer's instructions.]

Each school in the District shall have at least two (2) epinephrine **delivery systems auto-injectors (EpiPens)** available at the school site. It shall be the responsibility of the School Nurse to be sure that the supply of **delivery systems EpiPens** is maintained at the appropriate level and they have not expired. The Assistant Superintendent **of /Chief Financial Officer,** Personnel & Student Services shall also be responsible for coordinating the training of District employees to administer **delivery systems EpiPen injections** and to maintain the list of employees authorized to administer such **systems injections**.

Individuals Qualified to Administer

Only a licensed, registered professional nurse employed or contracted by the District or a school employee who has successfully passed the required training shall be allowed to possess and administer **epinephrine delivery systems EpiPen-injections** to students. The persons authorized to use the District maintained **epinephrine delivery systems EpiPen's** will be trained annually by the school nurse.

Each school shall have at least **(1)** one person trained in the appropriate use and administration of an **epinephrine delivery system EpiPen-injection**. In each school with ten (10) or more combined instructional and administrative staff, at least two (2) employees at that site shall be appropriately trained in the use of **an epinephrine delivery systems EpiPen**.

Training of employees on the appropriate use and administration of epinephrine delivery system ~~an EpiPen injection~~ shall be done in accordance with any guidelines provided by the Michigan Department of Education, and shall be conducted under the supervision of a licensed registered professional nurse. The training shall include an evaluation by the nurse of the employees' understanding of the protocols for administering epinephrine delivery system ~~an EpiPen injection~~.

Students to Whom Epinephrine Injections May Be Administered

A licensed, registered, professional nurse or trained and authorized employees under this policy may administer epinephrine delivery systems ~~EpiPen injections~~ to 1) any student who has a prescription on file with the District, in accordance with the directives in such prescription, and 2) any individual on school grounds who is believed to be having an anaphylactic reaction.

The District and its personnel are immune from civil and criminal liability related to the administration or non-administration of epinephrine to the extent set forth in applicable State law.

Reporting of Epinephrine Delivery Injections

Any person who administers an epinephrine delivery system ~~EpiPen injection~~ to a student shall immediately contact 911. Then promptly notify the building principal, who shall be responsible for promptly notifying the student's parent/guardian that epinephrine ~~an injection~~ has been administered.

All epinephrine delivered ~~EpiPen injections~~ by District employees to students shall be reported in writing to the Assistant Superintendent of Personnel & Student Services. The report shall include whether the school's or student's epinephrine delivery system ~~EpiPen~~ was used, how many injections were given, and whether the student was previously known to be subject to severe allergic reaction (anaphylaxis).

The Assistant Superintendent of Personnel & Student Services shall at least annually report to the Department of Education, in the form and manner determined by the Department, information on the number of epinephrine delivery systems ~~injections~~ provided to students, the number of uses ~~injections~~ with District epinephrine delivery systems ~~EpiPens~~ and the number of incidents where students were not known to be subject to severe allergic reactions.

T.C. 8/28/23

© Neola 2025 6

Legal

M.C.L. 380.1178, 380.1179, 380.1179A

Michigan Department of Education, Model Policy and Guidelines for Administering
Medications to Pupils at School

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po7540.03

STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY Revised

ADOPTED Jan 28, 2008 · REVISED Jun 12, 2023

7540.03 - STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

Technology directly affects the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt their means and methods of instruction and the way they approach student learning to incorporate the latest technologies. The Board of Education provides Information & Technology Resources (as defined in Bylaw 0100) (collectively, "District Information & Technology Resources") to support the educational and professional needs of its students and staff. With respect to students, District Information & Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students. The District's computer network and Internet system do not serve as a public access service or a public forum and the Board imposes reasonable restrictions on its use consistent with its stated educational purpose.

The Board regulates the use of District Information & Technology Resources in a manner consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. This policy, and its related administrative guidelines and the Student Code of Conduct, govern students' use of District Information & Technology Resources and students' personal communication devices when they are connected to District Information & Technology Resources, including online educational services/apps, regardless of whether such use takes place on or off school property (see Policy 5136).

Students are prohibited from using District Information & Technology Resources to engage in illegal conduct (e.g., libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, etc.) or conduct that violates this Policy and its related administrative guidelines and the Student Code of Conduct (e.g., making personal attacks or injurious comments, invading a person's privacy, etc.). Nothing herein, however, shall infringe on students' First Amendment rights. Because its Information & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Students have no right or expectation to privacy when using District Information & Technology Resources (including, but not limited to, privacy in the content of their personal files, messages/e-mails, and records of their online activity).

While the Board uses various technologies to limit students using its Information & Technology Resources to only use/access online educational services/apps and resources that have been pre-approved for the purpose of instruction, study, and research related to the curriculum, it is impossible to prevent students from accessing and/or coming in contact with online content that has not been pre-approved for use by students of certain ages. It is no longer possible for educators and community members to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to approved guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them) when significant portions of students' education take place online or through the use of online educational services/apps.

Pursuant to Federal law, the Board implements technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using District Information & Technology Resources if such disabling will cease to protect against access to materials that are prohibited under the CIPA. Any student who attempts to disable the technology protection measures will be disciplined.

The Superintendent or Director of Technology may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been mistakenly, improperly, or inadvertently blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

Parents are advised that a determined user may be able to gain access to online content and/or services/apps that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to content that they and/or their parents may find inappropriate, offensive, objectionable, or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

Principals are responsible for providing training so that students under their supervision are knowledgeable about this policy and its accompanying guidelines.

Pursuant to Federal law, students shall receive education about the following:

- A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
- B. the dangers inherent with the online disclosure of personally identifiable information;
- C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students online;
- D. unauthorized disclosure, use, and dissemination of personal information regarding minors

Staff members shall provide guidance and instruction to their students regarding the appropriate use of District Information & Technology Resources and online safety and security as specified above. Additionally, such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with others on social media and in chat rooms and cyberbullying awareness and response. Furthermore, staff members will monitor the online activities of students while they are at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions, or use of specific monitoring tools to review browser history and network, server, and computer logs.

All students who use District Information & Technology Resources (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines (Acceptable Use Policy).

In order to keep District Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, students are required to comply with all District-established cybersecurity procedures including, but not limited to, the use of multi-factored authentication for which they have been trained. Principals are responsible for providing such training on a regular basis and measuring the effectiveness of the training.

Students will be assigned a District-provided school e-mail account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, individuals, and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned e-mail account when signing up/registering for access to various online educational services/apps.

Students are responsible for good behavior when using District Information & Technology Resources – i.e., behavior comparable to that expected of students when they are in

physical classrooms and school buildings and at school-sponsored events. Because communications on the Internet are often public in nature, general school rules for behavior and communication apply. The Board does not approve any use of its Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students may only use District Information & Technology Resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

Expectations for Responsible Artificial Intelligence ("AI") Use

Students are strictly prohibited from inputting Personally Identifiable Information ("PII"), confidential student or staff data, or any non-public school records into any AI tool or service that has not been explicitly approved and contracted with by the District.

Students are expected to adhere to principles of transparency, proper citation, and responsible use of AI in all academic and school-related activities. Students must disclose the use and extent of AI assistance on any submitted work as required by staff.

Students are prohibited from using technology and/or AI to bully, harass, threaten, impersonate, or create or distribute deceptive or harmful content, including deepfake or synthetic media that falsely depicts another person. AI may not be used for academic dishonesty, privacy violations, or any conduct that materially disrupts the educational environment. Violations of this policy will result in disciplinary action consistent with Policy 5500 - Student Conduct, and other applicable Board policies.

Use of AI to Generate any Synthetic Intimate Representation

Any student suspected of using AI or other technological means to create a synthetic intimate representation will be referred to law enforcement in addition to any disciplinary action imposed by administration. Synthetic Intimate Representation means a representation generated using technological means that uses an identifiable person's face, likeness, or other distinguishing characteristic to depict an intimate representation of that person, regardless of whether the representation includes components that are artificial, legally generated, or generally accessible, and that is so realistic that a reasonable person would believe it depicts conduct of the identifiable person.

Academic Honesty

All student use of AI technology must comply with the requirements and standards set forth in Policy 7540.09 – Artificial Intelligence (AI).

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked and disciplinary action taken against them. Users are

personally responsible and liable, both civilly and criminally, for uses of District Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Technology Director as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Information & Technology Resources.

Cross Reference

po5500 - STUDENT CONDUCT

Revised 3/8/10

Revised 5/23/11

Revised 5/29/12

Revised 12/15/14

Revised 12/18/17

© Neola 2023 6

Legal

P.L. 106-554, Children's Internet Protection Act of 2000

P.L. 110-385, Title II, Protecting Children in the 21st Century Act

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6777, 9134 (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

47 C.F.R. 54.500 - 54.523



10-12-26 POLICY COMMITTEE SEPT UPDATE

po7540.04

STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY Revised

ADOPTED Jan 28, 2008 · REVISED Jun 12, 2023

7540.04 - **STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Technology directly affects the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt their means and methods of instruction and the way they approach student learning to incorporate the latest technologies. The Board of Education provides District Information & Technology Resources (as defined by Bylaw 0100) (collectively, "District Information & Technology Resources") to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's computer network and Internet system do not serve as a public access service or a public forum and the Board imposes reasonable restrictions on its use consistent with its stated educational purpose.

The Board regulates the use of District Information & Technology Resources by principles consistent with applicable local, State, and Federal laws and the District's educational mission. This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staff's use of the District's Information & Technology Resources and staff's personal communication devices when they are connected to District Information & Technology Resources, including online educational services/apps, regardless of whether such use takes place on or off school property (see Policy 7530.02).

Staff members are prohibited from using District Information & Technology Resources to engage in illegal conduct (e.g., libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, etc.) or conduct that violates this Policy and its related administrative guidelines (e.g., making personal attacks and injurious comments, invading a person's privacy, etc.). Nothing herein, however, shall infringe on a staff member's First Amendment rights. Because District Information & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Staff members have no right or expectation to privacy when using District Information & Technology Resources (including, but not limited to, privacy in the content of their personal files, messages/e-mails, and records of their online activity).

Staff are expected to use District Information & Technology Resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource-sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services/apps will be guided by Board Policy 2521 – Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that brings incredible education and information resources to our students. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District Information & Technology Resources provide students and staff with the opportunity to communicate with people throughout the world. Access to such an incredible quantity and diversity of information and resources brings with it, however, certain unique challenges and responsibilities.

While the Board uses various technologies to limit the use of District Information & Technology Resources to only use/access online services/apps and resources that have been pre-approved for the purpose of instruction, study, and research related to the curriculum, it is impossible to prevent users from accessing and/or coming in contact with online content that has not been pre-approved for use by students of certain ages. It is no longer possible for educators and community members to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them) when significant portions of students' education take place online or through the use of online educational services/apps.

Pursuant to Federal law, the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the District Information & Technology Resources if such disabling will cease to protect against access to materials that are prohibited under (CIPA). Any staff member who attempts to disable the technology protection measures without the

express written consent of an appropriate administrator will be disciplined, up to and including termination.

The Superintendent or Director of Technology may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Superintendent or Director of Technology may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Principals are responsible for providing training so that staff under their supervision are knowledgeable about this policy and its accompanying guidelines.

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

- A. the safety and security of students while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
- B. the inherent danger of students disclosing personally identifiable information when using AI and when online;
- C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students or staff online; and
- D. unauthorized disclosure, use, and dissemination of personal information regarding minors.

Staff members shall provide guidance and instruction to their students regarding the appropriate use of District Information & Technology Resources and online safety and security as specified above. Additionally, such training shall include, but not be limited to, education concerning appropriate online behavior including interacting with others on social media and in chat rooms and cyberbullying awareness and response. Further, staff members shall monitor students' online activities while the students are at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

All staff members who use District Information & Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its

accompanying guidelines. (Staff Acceptable Use Policy)

In order to keep District Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, staff members are required to comply with all District-established cybersecurity procedures including, but not limited to, the use of multi-factored authentication (MFA) for which they have been trained. Principals are responsible for providing such training on a regular basis and measuring the effectiveness of the training.

Staff will be assigned a District-provided school e-mail address that they are required to use for all school-related electronic communications, including those to students, parents, and other staff members.

With prior approval from the Superintendent or Director of Technology, staff may direct students who have been issued school-assigned e-mail accounts to use those accounts when signing up/registering for access to various online educational services/apps that the student will use for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District Information & Technology Resources - i.e., behavior comparable to that expected when they are in physical classrooms, school buildings, and at school-sponsored events. Because communications on the Internet are often public in nature, general rules for professional behavior and communication apply. The Board does not approve any use of District Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Staff members may only use District Information & Technology Resources to access or use social media if it is done for educational or business-related purposes.

Staff member use of District Information & Technology Resources to access or use social media is to be consistent with Policy 7544 and its accompanying procedure.

Social Media Use

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property, including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

Use of Artificial Intelligence/Natural Language Processing Tools

Staff are permitted to use Artificial Intelligence (AI) and Natural Language Processing (NLP) tools (collectively, “AI/NLP tools”) to accomplish their job responsibilities so long as the use is ethical, responsible, and does not violate any provisions of this policy (e.g., it does not infringe on students’ or staff members’ privacy rights, violate their duty to maintain confidentiality related to personally identifiable information, etc.).

With respect to students, it is the Board’s policy that they are required to rely on their own knowledge, skills, and resources when completing school work. In order to ensure the integrity of the educational process and to promote fair and equal opportunities for all students, except as outlined below, students are prohibited from using AI/NLP tools to complete school work. The use of AI/NLP tools without the express permission/consent of a teacher is considered to undermine the learning and problem-solving skills that are essential to a student’s academic success and that the staff is tasked to develop in each student. Consequently, students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI/NLP tools, and they are expected to ask their teachers when they have questions and/or need assistance. A student’s unauthorized use of AI/NLP tools is considered a form of plagiarism and any student found using such tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code of Conduct.

Notwithstanding the preceding, students are allowed to use AI/NLP tools in the school setting if they receive prior permission/consent from their teacher, so long as they use the AI/NLP tools in an ethical and responsible manner. Teachers have the discretion to authorize students to use AI/NLP tools for the following uses:

- A. **Research assistance:** AI/NLP tools can be used to help students quickly and efficiently search for and find relevant information for their school projects and assignments.
- B. **Data Analysis:** AI/NLP tools can be used to help students to analyze, understand, and interpret large amounts of data, such as text documents or social media posts. This can be particularly useful for research projects or data analysis assignments – e.g., scientific experiments and marketing research.
- C. **Language translation:** AI/NLP tools can be used to translate texts or documents into different languages, which can be helpful for students who are learning a new language or for students who are studying texts written in a different language.
- D. **Writing assistance:** AI/NLP tools can provide grammar and spelling corrections, as well as suggest alternative word choices and sentence structure, to help students improve their writing skills.
- E. **Accessibility:** AI/NLP tools can be used to help students with disabilities access and understand written materials. For example, text-to-speech software can help students with specific learning disabilities or visual impairments to read texts and

AI-powered translation tools can help students with hearing impairments to understand spoken language.

As outlined above, under appropriate circumstances, AI/NLP tools can be effectively used as a supplement to and not a replacement for traditional learning methods. Consequently, with prior teacher permission/consent, students can use AI/NLP tools to help them better understand and analyze information and/or access course materials. If a student has any questions about whether they are permitted to use AI/NLP tools for a specific class assignment, they should ask their teacher.

Authorized and Appropriate Use of Artificial Intelligence ("AI")

Staff are expected to use District-approved AI tools responsibly and ethically to support essential professional functions including, but not limited to, instruction, providing student feedback, and improving workflow efficiency.

All use of AI technology by staff must adhere to the requirements and standards detailed in Policy 7540.09 – Artificial Intelligence ("AI") .

Use of AI to Generate any Synthetic Intimate Representation

Any staff member or student suspected of using AI or other technological means to create a synthetic intimate representation will be referred to law enforcement in addition to any disciplinary action imposed by administration. Synthetic Intimate Representation means a representation generated using technological means that uses an identifiable person's face, likeness, or other distinguishing characteristic to depict an intimate representation of that person, regardless of whether the representation includes components that are artificial, legally generated, or generally accessible, and that is so realistic that a reasonable person would believe it depicts conduct of the identifiable person.

AI Prohibited Data Input

Staff shall use AI tools responsibly, ethically, and in compliance with District technology, student records, and data privacy policies.

Staff must not enter student Personally Identifiable Information ("PII"), staff PII, or proprietary District data into any AI system or service unless it has been explicitly reviewed, approved, and contracted by the District.

Staff members are prohibited from using AI tools to bully, harass, threaten, impersonate, or create or distribute deceptive or harmful content, including deepfake or synthetic media that falsely depicts another person. AI may not be used in ways that violate student or

employee privacy, compromise confidential information, engage in academic or professional misconduct, or otherwise disrupt the educational environment.

Any misuse of AI that violates Board policy, professional standards, or applicable law may result in disciplinary action, up to and including termination of employment.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff member use of District Information & Technology Resources.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality and/or privacy laws related to the disclosure of student or employee personally identifiable information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

Revised 3/8/10

Revised 5/23/11

Revised 5/29/12

Revised 12/15/14

Revised 12/18/17

© Neola 2023 6

Legal

P.L. 106-554, Children's Internet Protection Act of 2000

P.L. 110-385, Title II, Protecting Children in the 21st Century Act

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6777, 9134 (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

47 C.F.R. 54.500 – 54.523

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45



10-12-26 POLICY COMMITTEE SEPT UPDATE

po8310

PUBLIC RECORDS Revised

ADOPTED Jan 28, 2008 · REVISED Dec 15, 2021

8310 - PUBLIC RECORDS

The Board of Education recognizes its responsibility to maintain the public records of this District and to make such records available to residents of Michigan for inspection and reproduction.

The public records of this District include any writing or other means of recording or retaining meaningful content prepared, owned, used, in the possession of, or retained by the District, its Board, officers, or employees, subject to certain exemptions according to the Michigan Freedom of Information Act (FOIA). The District shall not disclose the confidential address of a student or of an employee who has provided proper notice of a participation card issued by the department of the attorney general under the address confidentiality program act.

Any record, or portion thereof, generated or compiled by an Artificial Intelligence ("AI") system and/or social media/PCD communications between students and Board members, staff, and/or volunteers are subject to all provisions of this policy and all other applicable Board policies, ~~() administrative guidelines,~~ [END OF OPTION] and State or Federal laws. The District maintains full and sole responsibility for the accuracy, security, access, and disclosure of all AI-generated content within a student's education record, as if the content were created solely by a District employee.

Any person may make a written request for any public records of the District. The person may inspect, copy, or receive copies of the public record requested. The District shall respond to such requests within five (5) working days after receipt unless otherwise agreed to in accordance with the Freedom of Information Act.

An individual may purchase copies of the District's public records upon payment of a fee. No original public record may be removed from the office in which it is maintained except by a Board officer or employee in the course of the performance of their ~~his/her~~ duties.

Neither the Board nor its employees shall permit the release of the social security number of an employee, student, or other individual except as authorized by law (see Policy 8350 and AG 8350).

The Board authorizes the Superintendent to provide, upon written request, enhanced i.e. immediate access to any public record, which the District has stored in an electronic database and is not confidential or exempt from disclosure by State or Federal statute. Such a record may be provided by means of a computer disk provided by the requestor, electronic mail, or a modem providing the requestor has paid the fee established for such transmission.

The Board has determined that personal and confidential information provided to and retained by the District on parents, students, staff and others will be considered exempt from disclosure pursuant to a Freedom of Information Act request, unless advised specifically by the District's legal counsel that the particular information must be released. Such personal and confidential information shall include home addresses, telephone numbers, e-mail addresses or website pages (e.g. My Space, Facebook), except as they are specifically related to the operation of the schools, or specifically authorized for release by the individual, or the parent/guardian if the individual is a minor.

Nothing in this policy shall be construed as preventing a Board member from inspecting in the performance of their ~~his/her~~ official duties any record of this District, except student records and certain portions of personnel records.

The Superintendent is authorized to dispose of correspondence on a daily basis including those transmitted by means of voice mail or E-mail, providing the message does not alter existing District records.

The Superintendent is responsible for transmission of data contained in the single record student database established by the Michigan Department of Education. Such transmission shall be in accordance with procedures established by the Livingston Education Service Agency and the Center for Educational Performance and Information (CEPI).

The Superintendent shall establish administrative guidelines to ensure proper compliance with the intent of this policy and the Freedom of Information Act.

Revised 9/28/09

© Neola 202 1 6

Legal

M.C.L. 15.231 et seq.

M.C.L. 445.81 et seq.

Michigan Federation of Teachers v. University of Michigan, 481 Mich. 657 (2008)



10-12-26 POLICY COMMITTEE SEPT UPDATE

po8321

CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY) Revised

ADOPTED Nov 26, 2012 · REVISED Feb 17, 2025

8321 - CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY)

The District is required by State law to have the Michigan State Police (MSP) obtain both a State and a Federal Bureau of Investigation (FBI) criminal history record information (CHRI) background check report for all employees of the District and contractors, vendors and their employees who work on a regular and continuous basis in the District. This policy provides the appropriate access, maintenance, security, confidentiality, dissemination, integrity, and audit requirements of CHRI in all its forms, whether at rest or in transit. This policy/procedure shall be reviewed and updated at least annually and following any security incidents involving CHRI. To assure the security, confidentiality, and integrity of the CHRI background check information received from the MSP/FBI, the following standards are established:

A. Sanctions for Non-Compliance

Employees who fail to comply with this policy, State and Federal law, current CJISSECPOL, rules or regulations, and any guidelines issued to implement this policy will be subject to discipline for such violations. Discipline can range from counseling and retraining to discharge and prosecution, based on the nature and severity of the violation, at the District's discretion. All violations will be recorded in writing, with the corrective action taken. The Superintendent shall review, approve, sign, and date all such corrective actions.

B. Local Agency Security Officer (LASO)

The Assistant Superintendent of Personnel and Student Services shall be designated as the District's Security Officer ("LASO"). The LASO shall be an employee most directly involved in the fingerprint/background check process. The LASO is an authorized user/personnel, has completed a fingerprint-based background check where required, and has been found appropriate to access CHRI, and an employee directly involved in evaluating an individual's qualifications for employment or assignment. The LASO shall be responsible for overall implementation of this policy and for data and system security. This shall include:

1. identifying who is using or accessing CHRI and/or systems with access to CHRI;
2. identifying and documenting any equipment connected to the State system;
3. ensuring that personnel security screening procedures are being followed as set forth in this policy;
4. ensuring that approved and appropriate security measures are in place and working as expected;
5. supporting policy compliance and instituting the incident response reporting procedures;
6. ensuring annual awareness and training is being completed by all personnel with authorized access to the CHRI;
7. ensuring that the Michigan State Police are promptly informed of any security incidents involving the abuse or breach of the system and/or access to criminal justice information;
8. reviewing and updating information security policy/procedures annually or after security incidents involving CHRI;
9. employing one (1) or more of the following techniques to increase the security and privacy awareness of system users: displaying posters, offering supplies inscribed with security and privacy reminders; displaying logon screen messages; generating email advisories or notices from organizational officials; conducting awareness events; and
10. to the extent applicable, identifying who is using the Michigan State Police approved hardware, software and firmware, and ensuring that no unauthorized individuals have access to these items.

The District's LASO shall be the point of contact for the Michigan State Police and should be the person most knowledgeable about this policy. The District's LASO shall be designated on the appropriate form as prescribed and maintained by the Michigan State Police. A new form shall be submitted every time a new LASO is designated and kept on file by the District indefinitely.

Privacy Act Statement Disclosure

The District shall ensure that the applicant receives the Federal Privacy Act Statement Disclosure by providing the applicant with the most current

version of the MSP RI-030 Live Scan consent form. The applicant will receive this information by hard or electronic copy.

C. Agency User Agreements

The District shall enter into any required User Agreement for Release of CHRI ("User Agreement"), and future amendments, by the Michigan State Police necessary to access the required CHRI on applicants, volunteers, and all other statutorily required individuals, such as contractors and vendors and their employees assigned to the District. Agreements are in place to provide data ownership, individual roles, responsibilities, etc. The District shall request a new user agreement in the event they have a legal name change, they move to a new physical address, ~~or~~ they wish to add or remove fingerprint reason codes, or when the District's signatory changes. The most current copy of the Agreement shall be maintained on file at the agency indefinitely. The LASO shall be responsible for the District's compliance with the terms of any such User Agreement.

D. Personnel Security

Authorized users/personnel shall be individuals who have been appropriately vetted through a national fingerprint-based background check, as required by school safety legislation, and have been granted access to CHRI data, wherein access is only for the purpose of evaluating an individual's qualifications for employment or assignment.

1. **Subsequent Arrest/Conviction** - If an individual granted access to criminal justice information is subsequently arrested and/or convicted, access shall be suspended immediately until the matter is reviewed by the LASO to determine if continued access is appropriate. Such determination shall be recorded in writing, signed, dated, and maintained with the individual's file. In the event that the LASO has the arrest/conviction, the Superintendent (if not the designated LASO) shall make the determination. If the Superintendent is also the designated LASO, the determination shall be made by the Assistant Superintendent of Personnel and Student Services. Except that, as noted in D(1)(a), individuals with a felony conviction of any kind will have access indefinitely suspended.
2. **Public Interest Denial** - If the LASO determines that access to criminal justice information by any individual would not be in the public interest, access shall be denied whether that person is seeking access or has previously been granted access. Such decision and reasons shall be in writing, signed, dated, and maintained in the individual's file.
3. **Approval for Access** - All requests for access to criminal justice information shall be as specified and approved by the LASO. Any such designee must be a

direct employee of the District. The District must maintain a readily accessible list that includes the names of all LASO-approved personnel with access to criminal justice information, as well as the reason for providing each individual access. This list shall be made available to the Michigan State Police upon request.

4. **Notification of Termination of Employment/Access or Transfer/Re-assignment** - When an employee's access or employment is terminated, or if the duties for accessing criminal justice information have been transferred or re-assigned to another individual, the Assistant Superintendent of Personnel shall be notified promptly in writing. The individual responsible for the termination or transfer/re-assignment shall directly notify the Superintendent.

5. **Termination of Employment/Access** - Within twenty-four (24) hours of the termination of employment, all access to criminal justice information shall be terminated immediately for that individual, such as requiring the individual to return any keys or access cards to buildings, offices, and/or files, or closing the individual's account and/or blocking access to any systems containing such information at the District.

6. **Transfer/Re-assignment** - When an individual who has been granted access to criminal justice information has been transferred or re-assigned to other duties, the LASO shall determine whether continued access is necessary and appropriate. If not, the LASO shall take such steps as necessary to block further access to such information within the twenty-four (24) hour period immediately following the transfer or reassignment. If such access is not necessary and appropriate, steps to eliminate the individual's access will be taken immediately, such as requiring the individual to return any keys or access cards to buildings, offices, and/or files, or closing the individual's account and/or blocking access to any systems containing such information at the District.

E. Media Protection

Access to digital and physical media in all forms, which contains criminal history background information provided by the Michigan State Police through the statutory record check process, is restricted to authorized individuals only. Only individuals involved in the hiring determination of both District employees and volunteers shall be authorized to access digital and physical media containing CHRI.

1. **Media Storage and Access** - All digital and physical media shall be stored in a physically secure location or controlled area, such as locked office, locked cabinet or other similarly secure area(s) which can only be accessed by authorized individuals. If such security cannot be reasonably provided, then

all digital CHRI background data shall be encrypted. Access to such media will be secured at all times when not in use or under the supervision of an authorized individual. Digital media shall be stored on a District or School server, and unless encrypted, shall be maintained in a lockable filing cabinet, drawer, closet, office, safe, vault, etc. Storage on a third party server, such as cloud service, is not permitted. Storage of digital media must conform to the requirements in AG 8321 and must be encrypted. Physical media will be stored within individual records when feasible, or by itself when necessary, and will be maintained in a lockable filing cabinet, drawer, closet, office, safe, vault, etc.

2. **Media Transport** – Digital and physical media shall only be transported upon sufficient justification approved by the LASO. Digital and physical media shall be protected when being transported outside of a controlled area. Only authorized individuals shall transport the media. Physical media (e.g. printed documents, printed imagery, etc.) shall be transported using a locked container, sealed envelope, or other similarly secure measure. To the extent possible, digital media (e.g., hard drives and removable storage devices such as disks, tapes, flash drives and memory cards) shall be either encrypted and/or be password protected during the transport process. The media shall be directly delivered to the intended person or destination and shall remain in the physical control and custody of the authorized individual at all times during transport. Access shall only be allowed to an authorized individual.

3. **Media Disposal/Sanitization** – When the CHRI background check is no longer needed, the media upon which it is stored shall either be destroyed or sanitized. The LASO and the Superintendent shall approve in writing the media to be affected. CHRI records This record shall be maintained by the LASO during the individual's active employment plus an additional six (6) years.

[DRAFTING NOTE: The regulations do not specify a specific period for maintaining this information. This time period is suggested based on the State of Michigan's background information retention schedule and will likely cover most statutes of limitation and can be retained in digital format.]

a. **Digital Media** - Sanitization of the media and deletion of the data shall be accomplished by either overwriting at least three (3) times or by degaussing, prior to disposal or reuse of the media, but optical media (such as CDs and DVDs) will be physically destroyed. If the media is inoperable or will not be reused, it shall be destroyed by shredding, cutting, or other suitable method to assure that any data will not be retrievable.

b. **Physical Media** – Disposal of documents, images or other type of physical record of the criminal history information shall be cross-cut shredded or incinerated. Physical security of the documents and their information shall be maintained during the process by authorized individuals. Documents may not be placed in a wastebasket or burn bag for unauthorized individuals to later collect and dispose of.

c. **CHRISS Unsubscription** – All records shall be unsubscribed in CHRISS within five (5) business days to ensure timely removal from rap back notifications.

All disposal/sanitization shall be either conducted or witnessed by authorized personnel to assure that there is no misappropriation of, or unauthorized access to, the data to be deleted. As a best practice, ~~w~~ **W**ritten documentation of the steps taken to sanitize or destroy the media should ~~shall~~ be maintained for ten (10) years, and must include the date as well as the signatures of the person(s) performing and/or witnessing the process. (See also, AG 8321.)

4. **Personal Mobile Devices** – A personally owned mobile device (mobile phone, tablet, laptop, etc.) or no identifiable owner digital media device shall not be authorized to access, process, store or transmit criminal justice information unless the District has established and documented the specific terms and conditions for personally owned mobile devices through a Mobile Device Management (MDM) system. An MDM is not required when receiving CHRI from an indirect access information system (i.e., the system provides no capability to conduct transactional activities on State and national repositories, applications, or services).

5. **CHRI Background Check Consent and Documentation**

All individuals requested to complete a fingerprint-based CHRI background check must execute Michigan State Police Form RI-088A at the time of application and be notified fingerprints will be used to check the criminal history records of the FBI, prior to completing a fingerprint-based CHRI background check. The most current and unaltered Live-scan form (RI-030) will satisfy this requirement and must be retained. Individuals subject to a fingerprint-based CHRI background check shall be provided the opportunity to complete or challenge the accuracy of the individual's criminal history record.

~~Some type of documentation identifying the position for which a fingerprint-based CHRI background check has been obtained must be retained for every CHRI background check conducted, such as the "Agency User Agreement" (RI-~~

087); an offer letter, employment agreement, new hire checklist, employment contract, volunteer background check form, etc.

6. **Controlled Area/Physical Protections**

All CHRI obtained from the Michigan State Police pursuant to the statutorily required background checks shall be maintained in a physically secure and controlled area, which shall be a designated office, room, or area. The following security precautions will apply to the controlled area:

- a. Limited unauthorized personnel access to the area during times that criminal justice information is being processed or viewed.
- b. The controlled area shall be locked at all times when not in use or attended by an authorized individual.
- c. Information systems devices (e.g., computer screens) and physical documents, when in use, shall be positioned to prevent unauthorized individuals from being able to access or view them.
- d. Encryption shall be used for digital storage of criminal justice information. (See AG 8321)

7. **Passwords (Standard Authentication)¹**

All authorized individuals with access to computer or systems where processing is conducted or containing criminal justice information must have a unique password to gain access. This password shall not be used for any other account to which the individual has access and shall comply with the following attributes and standards:

- a. at least eight (8) characters long on all systems
- b. not be a proper name or a word found in the dictionary
- c. not be the same as the user identification
- d. not be displayed when entered into the system (must use feature to hide password as typed)
- e. not be transmitted in the clear outside of the secure location used for criminal justice information storage and retrieval

f. must expire and be changed every ninety (90) days

g. renewed password cannot be the same as any prior ten (10) passwords used (See also, AG 8321)

8. Security Awareness Training

All individuals who are authorized by the District to have access to criminal justice information or to systems which store criminal justice information shall have basic security awareness training as part of initial training for new users prior to accessing CJI and annually thereafter, and when required by system changes or within thirty (30) days of any security event for individuals involved in the event. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

Training is a role-based security and privacy training for personnel with the following roles:

a. **Basic Role:** All individuals with unescorted access to a physically secure location. (Not typical for NCJAs)

b. **General Role:** All personnel with access to CJI. This level is designed for people who have physical and logical access to CJI.

c. **Privileged Role:** This level is designed for all information technology personnel including system administrators, security administrators, network administrator, etc. More access is needed than a general user, but not an assigned LASO. (i.e., CHRISS Administrator)

d. **Security Role:** This level is designed for personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. (i.e., LASO)

The training shall, to the extent possible, be received through a program approved by the Michigan State Police. A template of the training is provided on the Michigan State Police's website. At a minimum, the training shall comply with the standards established by the U.S. Department of Justice and Federal Bureau of Investigation for Criminal Justice Information Services. (See AG 8321.) A record shall be kept current of all individuals who have completed the security awareness training.

9. Secondary Dissemination of Information

If criminal history background information received from the Michigan State Police is released to another authorized agency under the sharing provision

designated by the revised school code, a log of such releases shall be maintained and kept current for all dissemination outside of the CHRIS system indicating:

- a. the date of release;
- b. record disseminated;
- c. method of sharing;
- d. agency personnel that shared the CHRI;
- e. the agency to which the information was released;
- f. the name of the individual recipient at the agency; and
- g. whether authorization was obtained.

A log entry need not be kept if the receiving agency/entity is part of the primary information exchange agreements between the District and the Michigan State Police. A release form consenting to the sharing of CHRI shall be maintained at all relevant times.

If CHRI is received from another District or outside agency, an Internet Criminal History Access Tool (ICHAT) background check shall be performed to ensure the CHRI is based on personal identifying information, including the individual's name, sex, and date of birth, at a minimum.

Incident Handling and Responses

The District shall establish operational incident handling procedures for instances of an information security breach. Information security incidents are major incidents that significantly endanger the security or integrity of CHRI. The District will identify responsibilities for information security incidents and include how and who to report such incidents to. The District will ensure appropriate security incident capabilities exist and should incorporate the lessons learned from ongoing incident handling activities. The District will ensure procedures exist and are implemented for a follow-up action of a security breach and for the collection of evidence in cases of legal action. All individuals with direct or indirect access to CHRI shall be trained on how to handle an information security incident, and such training will be included within the provided awareness and training. Information system security incidents shall be tracked using Form CJIS-016 and documented on an ongoing basis. Incident-related information may be obtained from audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The LASO shall maintain completed security incident reporting forms for three (3) years or until legal action (if warranted) is complete, whichever timeframe is greater. The

District shall implement steps for incident handling capabilities, for both digital and physical CHRI media. Incident response testing will be conducted annually using the following tests: tabletop or walk-through exercises, simulations, or other agency appropriate tests. At a minimum, the following will be implemented:

	Physical - Hard Copy CHRI	Digital - Digitally Saved CHRI
1. Preparation	The CHRI container will be locked at all times in the business office where it is stored. The office must be locked when the office staff is not present.	Firewalls, virus protection, and/or malware/spyware protection shall be implemented and maintained to prevent unauthorized access or intrusion of the information systems.
2. Detection	Unauthorized activities or physical intrusions to the building shall be monitored by building alarm or video surveillance. Doors must be locked and checked at night.	Electronic intrusions shall be monitored and detected by the firewalls, virus protection, and/or malware/spyware protection software.
3. Analysis	The LASO will work with police authorities to determine how the incident occurred and what data was affected.	The LASO shall work with the IT department to determine what systems or data were compromised and affected.
4. Containment	The LASO shall lock uncompromised CHRI information in a secure container, or transport CHRI to a secure area.	The IT department shall stop the spread of any intrusion of the information systems and prevent further damage.
5. Eradication	The LASO shall work with law enforcement to remove any threats and compromised CHRI data.	The IT department shall remove the intrusion of the information systems before restoring the system. All steps necessary to prevent recurrence shall be taken before restoring the system.

6. Recovery	The Police shall handle and/or oversee the recovery of stolen CHRI media. The LASO may contact MSP for assistance in re-fingerprinting if necessary.	The IT department shall restore the agency information system and media to a safe environment.

When an incident involving the security of CHRI or systems with access to CHRI is discovered, the following procedures shall be followed:

- A. All personnel are required to report suspected incidents to the LASO immediately, but not to exceed one (1) hour after discovery. Personnel who become aware of an incident or believe an incident has occurred should report to the following individuals, in order:
 1. LASO
 2. The Superintendent
- B. The breach shall be assessed (including determination of whether notification to individuals is needed, assessment of the extent of the harm, and identification of applicable privacy requirements) and steps taken to correct the situation:
 1. access shall be stopped for any unauthorized user;
 2. media shall be secured;
 3. systems shall be shut down as necessary to avoid further exposure to unauthorized access or dissemination of CHRI;
 4. such other steps are deemed necessary by the LASO or authorized personnel involved in assessing the incident.
- C. All necessary information regarding the security breach and District responses shall be recorded, analyzed, and preserved, including who was involved in taking incident response measures.
- D. The LASO shall be responsible for filing the incident report with the MSP using the CJIS-016. Completed CJIS-016 forms shall be retained on an ongoing basis to meet policy requirements for tracking..

The LASO shall monitor MSP information/guidance on incident reports and train authorized users with access to CHRI on detection and response to security incidents.

E. Mobile Device - Incident Handling and Response

1. The LASO shall be notified immediately.
2. The breach shall be assessed and steps taken to correct the situations:
 - a. access shall be stopped immediately, and remotely if necessary, for any authorized user;
 - b. media shall be secured and steps taken to identify how the incident occurred and what systems or data were compromised or affected;
 - c. systems shall be shut down as necessary to avoid further exposure to unauthorized access or dissemination of CJI;
 - d. such other steps as are deemed necessary by the LASO or authorized personnel involved in assessing the incident.
3. All necessary information regarding the security breach and District responses shall be recorded, analyzed, and preserved, including who was involved in taking incident response measures.
4. Steps shall be taken to restore the device and media to a safe environment.
5. The LASO shall be responsible for filing the incident report with the MSP using form CJIS-016. A copy of the completed form shall be retained and produced to MSP upon request.

When a device is lost the District shall document and indicate how long the device has been lost. Special reporting procedures for mobile devices shall apply in any of the following situations:

a. for a lost device, report if the owner:

1. believed the device was locked;
2. believed the device was unlocked;
3. could not validate the device's locked state.

b. for a total loss of a device, report if:

1. CHRI was stored on the device;
2. the device was locked or unlocked;
3. capable of remote tracking or wiping of device.

c. report any compromise of a device when the intrusion occurs while still in the owner's possession

d. report any compromise outside of the United States

F. Collection of Evidence

Where an information security incident involves legal action by or against the District or an individual (either civil or criminal), evidence shall be collected, retained, and presented in accordance with the rules of evidence of the relevant jurisdiction(s). For criminal matters, local law enforcement shall be contacted for evidence collection. For civil matters, Thrun Law Firm/district approved counsel will be contacted for evidence collection.

¹Applicable to districts that maintain CHRI within a digital system of records, such as a digital database, filing system, record keeping software, spreadsheets, etc. Not applicable if CHRI kept solely via e-mail and/or paper copies.

Revised 6/9/14

Revised 12/14/15

Revised 11/21/16

Revised 12/18/17

Revised 6/25/18

Revised 5/19/21

© Neola 2024 6

Legal

Ref: Criminal Justice Information Services - Security Policy (Version 5.6, 2017),

U.S. Dept. of Justice and Federal Bureau of Investigation

Noncriminal Justice Agency Compliance Audit Review, Michigan State Police, Criminal
Justice Information Center, Audit and Training Section

Conducting Criminal Background Checks, Michigan State Police, Criminal Justice
Information Center



10-12-26 POLICY COMMITTEE SEPT UPDATE

po8420

EMERGENCY SITUATIONS AT SCHOOLS Revised

8420 - EMERGENCY SITUATIONS AT SCHOOLS

The Board shall ensure that the District's emergency operations plans, emergency procedures, and crisis response protocols incorporate the Standardized Response Terminology established by the Michigan Department of State Police pursuant to M.C.L. 380.1308c.

The District shall utilize the following standardized emergency response terminology and actions:

1. Hold
2. Secure
3. Lockdown
4. Evacuate
5. Shelter

The Superintendent shall ensure that emergency plans, staff training, student instruction, and emergency drills utilize this standardized terminology in accordance with State law and any applicable administrative rules.

A. Emergency Preparedness

The District shall develop emergency preparedness procedures that address the following goals and/or objectives:

1. the health and safety of students and staff are safeguarded
2. the time necessary for instructional purposes is not unduly diverted
3. minimum disruption to the educational program occurs

4. students are helped to learn self-reliance and trained to respond sensibly to emergency situations

All threats to the safety of District facilities shall be identified by appropriate personnel and responded to promptly in accordance with the plan for emergency preparedness.

School personnel, including teachers, shall provide for unrestricted emergency egress during school hours and when the school is open to the public.

B. Drills

1. Each school shall conduct a minimum of five (5) fire drills each school year. Three (3) of the fire drills shall be held by December 1st of the school year, and two (2) shall be held during the remaining part of the school year, with a reasonable spacing interval between each drill.
2. Each school shall conduct a minimum of two (2) tornado safety drills each school year. At least one (1) of the tornado safety drills shall be conducted during March of the school year. These drills shall be conducted for the purpose of preventing injuries caused by severe weather.
3. Each school shall conduct a minimum of three (3) drills in which the occupants are restricted to the interior of the building and the building secured each school year. At least one (1) of these drills shall be conducted by December 1st of the school year, and at least one (1) shall be conducted after January 1st of the school year, with a reasonable spacing interval between each drill. Such drills shall include security measures that are appropriate to an emergency such as the release of a hazardous material or the presence of a potentially dangerous individual on or near the premises. The Superintendent shall seek input from local public safety officials on the nature of the drills to be conducted under this subsection.
4. Each school shall conduct at least one (1) of the drills required under Sections 2(A)-(C) during a lunch or recess period, or at another time when a significant number of the students are gathered but not in the classroom.
5. Schools shall not conduct a drill required under Sections 2(A)-(C) at a time that would interfere with the conduct of a state-mandated assessment.
6. Not later than September 15th of each school year, the Principal shall provide a list of the scheduled drill days to the county emergency management coordinator.

7. If a drill is not conducted on a scheduled drill day due to conditions not within the control of school authorities, such as severe storms, fires, epidemics, utility power unavailability, water or sewer failure, or health conditions as defined by the city, county, or State health authorities, the school shall reschedule the drill to occur within ten (10) school days after the scheduled date of the cancelled drill. The school's Principal shall notify the county emergency management coordinator of the rescheduled date for the drill.

C. Drill Result Publication

1. The Principal shall provide that documentation of a completed school safety drill is posted on the school's [or the District's] website within thirty (30) school days after the drill is completed and is maintained on the website for at least three (3) years.
2. The documentation posted on the website shall include at least all of the following:
 - a. name of the school
 - b. school year of the drill
 - c. date and time of the drill
 - d. type of drill completed
 - e. number of completed drills for that school year for each type of drill required under Sections 2(A)-(C)
 - f. signature of the school principal or his/her designee acknowledging the completion of the drill
 - g. name of the individual in charge of conducting the drill, if other than the school Principal

D. Cardiac Emergency Response Plan

The District shall adopt and implement a written Cardiac Emergency Response Plan for each school building, school grounds, and school-sponsored athletic events or organized athletic programs. The plan shall address and provide for:

1. The placement, regular maintenance, and inspection of automated external defibrillators ("AEDs") in unlocked, publicly accessible locations throughout

campus and athletic facilities, clearly marked with identifying signage. ~~Use and regular maintenance of automated external defibrillators, if available.~~

2. Activation of a cardiac emergency response team during an identified cardiac emergency.
3. A plan for effective and efficient communication throughout the school campus.
4. Ongoing training in CPR, AED use, and first aid for designated personnel (including high school athletic coaches), as well as annual exercise simulations to practice response protocols. ~~If the school includes grades 9 to 12, a training plan for the use of an automated external defibrillator and in cardiopulmonary resuscitation techniques.~~
5. Incorporation and integration of the local emergency response system and emergency response agencies with the school's plan.
6. An ongoing annual review and a comprehensive triennial evaluation of the Cardiac Emergency Response Plan. ~~An annual review and evaluation of the cardiac emergency response plan.~~

© Neola 20 ~~14~~ 26

Legal

M.C.L. 29.19

A.C. 1301:7-7-01, 3301-35-03 (D), 3301-83-15

HB No. 4713 (2013)