DEFOREST AREA SCHOOL DISTRICT

Draft - District Policies

Artificial Intelligence (AI) Special Update

11 policies

October 21, 2026

Table of Contents

01 - OVERVIEW	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 OVERVIEW
po5136	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised PERSONAL COMMUNICATION DEVICES
po5505	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised ACADEMIC HONESTY
po7440.02	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised SMART SENSOR AND MONITORING TECHNOLOGY
po7540	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised TECHNOLOGY
po7540.03	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
po7540.08	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised ARTIFICIAL INTELLIGENCE (AI)
po8310	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised PUBLIC RECORDS
po8315	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised PRESERVATION OF RECORDS AND LITIGATION HOLDS
po8330	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised STUDENT RECORDS
po8330.01	Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised UNAUTHORIZED ACQUISITION OF STUDENT PERSONAL INFORMATION

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

01 - OVERVIEW

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 OVERVIEW

WISCONSIN LOCAL UPDATE OVERVIEW AND COMMENTS

VOLUME 35 NUMBER 2 - Artificial Intelligence (AI)

JULY 2026

Artificial Intelligence Toolkit

Purpose & Overview The **attached** (to this Overview) toolkit and accompanying legally vetted policy templates guide district leaders in defining, implementing, and governing artificial intelligence (AI) within their local contexts. As AI evolves faster than statutory precedents, this resource enables leadership teams and boards to evaluate organizational capacity, mitigate compliance risks, and build a tailored strategy.

Implementation Framework Successful AI adoption requires a phased approach tailored to your District's size and capacity:

- **Immediate Focus:** Mitigate risk by training staff on the legal and privacy hazards of unvetted "Shadow AI" tools under FERPA, COPPA, and related statutes.
- **Sustained Growth:** Form representative AI workgroups or designate a key individual or individuals to manage long-term implementation and oversight.

Scope & Responsibilities This document serves as a planning guide, not a substitute for local legal counsel. Specific compliance questions must be reviewed by your district's legal team. Furthermore, this toolkit is not a rigid checklist, a data facilitation service, or a directory of pre-vetted software. Districts retain full responsibility for their implementation timelines, vendor selection, and the final legal vetting of all deployed AI tools.

The proposed new, revised, and replacement policies, administrative guidelines, and forms included in this update have been thoroughly prepared and reviewed by Neola's legal counsel for statutory compliance. If you make revisions or substitute in their entirety policies or other materials of your own drafting, those materials should be reviewed by

your legal counsel to verify compliance. Neola does not review District specific edits to update materials or District-specific policies for statutory compliance.

If a District chooses not to adopt a policy or administrative guideline, the District is still obligated to follow applicable Federal and State laws relating to that topic.

If a policy or guideline is marked as a revision, the revisions have been marked in bold (to add material) and crossed out (to delete material). As you review a revised policy or guideline, you may accept one, many, or all of the revisions provided. If a policy or guideline is marked as a replacement, enough revisions have been made to justify a complete, clean replacement copy. As you review a replacement policy or guideline, you should also check the materials you have in your current policy or guideline to see if there is some specific wording you want to be included in the replacement policy. If so, a copy of any wording to be added and where it should be inserted should be forwarded with the replacement policy or guideline when it is returned to the Coshocton office for processing.

If the District authors language and adds it to a policy template or deletes content that is not marked as a choice in the policy template, then these actions will constitute District-specific edits.

Policies to be deleted from the policy manual require Board action to rescind the policy.

Your Neola Associate will contact you soon to schedule an appointment to review this update and ensure you are current on it and previous updates.

If you are not an administrative guidelines client, you did not receive those materials in this packet. Contact your Associate for more information about becoming an administrative guidelines client.

Questions?

- All Neola Production-related materials and questions should be directed to the Coshocton Office at 632 Main Street, Coshocton, Ohio 43812 (phone: 800-407-5815 or email: production@neola.com). Billing questions should be directed to the Stow Office at 3914 Clock Pointe Trail, Suite 103, Stow, Ohio 44224 (phone 330-926-0514, fax 330-926-0525).

- Please direct questions related to content to your Neola Associate.

- Please make any revisions on the new Neola Policy Publishing Tool using the instructions provided to you. If you encounter anything unfamiliar in the Neola Policy Publishing Tool or have questions regarding the submission process, our support team is ready to help.

Call us: 330-926-0514

Email us: support@neola.com

Processing Update Materials

Revisions to your policies and administrative guidelines should be made using the new Neola Policy Publishing Tool, following the instructions provided.

District-Specific Materials

If the District chooses, during any step of the Update process, to incorporate District specific material into a new policy or guideline that has been proposed or to insert District-specific material into a current policy or guideline for which revisions have been proposed in an update issued by Neola, then the District agrees to hold Neola harmless for those District-specific edits and acknowledges that Neola's warranty for legal challenges to that District-specific language in that policy or guideline will not be in effect. In addition, Neola retains ownership of the text from the original policy template that remains in a policy to which District-specific material has been added. District-specific materials include the following:

1. Materials from the District's existing materials that the District requests be incorporated during the drafting process;

2. New materials that the District develops in their entirety and exclusive of Neola;

3. Revisions or deletions that substantively depart from Neola's templates; and

4. Outdated material that a District did not keep current with Neola updates.

Further, Neola does not recommend the use or incorporation of District-specific materials. Neola will, at the request of the District, incorporate District-specific materials into the licensed materials, with the implicit understanding that the District bears all risks associated with the District's decision to request that such District specific materials be incorporated. Neola reserves the right to but is not obligated to, advise the District to seek its own legal review of District-specific materials.

Notice Regarding Legal Accuracy

Neola is vigilant in providing policy language to clients that has been vetted for legal accuracy by outside legal counsel. Should questions arise as to the legal compliance or accuracy of Neola materials, it is our expectation that Neola's counsel would have the opportunity to assist in the resolution of such a claim. Please notify the Neola corporate office if an issue arises in which such a review or assistance is necessary.

Policies in this update have been reviewed by Renning Lewis & Lacy, s.c. for consistency with Federal and State law.

BYLAWS AND POLICIES

Policy 5136 - PERSONAL COMMUNICATION DEVICES (Revised)

This policy establishes a necessary regulatory framework to safeguard individual privacy, maintain academic integrity, and mitigate material disruptions to the instructional environment and conforms to statutory mandates, specifically Wis. Stat. § 120.12(29) and 2025 Wisconsin Act 42.

This update helps modernize the District's enforcement parameters by addressing emerging technologies, such as the integration of artificial intelligence. These changes are recommended but not required.

Policy 5505 - ACADEMIC HONESTY (Revised)

This policy is provides fair grading practices and standards of honesty expected of all students.

The updates are critical because they expand the definition of cheating to include modern violations, such as faking research data and using artificial intelligence to hide copied work. Finally, these changes protect student rights by requiring a full review of the facts, ensuring that automated AI software cannot be used as the sole reason to punish a student. These changes are recommended but not required.

Policy 7440.02 - SMART SENSOR AND MONITORING TECHNOLOGY (Revised)

This policy contributes to protecting the health and safety of the school community by authorizing the use of smart sensors to detect rule violations and security threats.

The updates are critical because they expand the District's oversight to include the use of Artificial Intelligence (AI) for monitoring and analyzing real-time video footage. Finally, these changes provide greater operational flexibility by allowing mobile tracking equipment and creating a new exception for authorized instructional uses. These changes are recommended but not required.

Policy 7540 - TECHNOLOGY (Revised)

This policy is provides guidance on the District's technology assets including information on how students and staff can use school networks and devices safely and ethically.

The updates are important because they officially recognize Artificial Intelligence (AI) tools as a fundamental part of the District's technology infrastructure. These changes require all AI software and hardware to meet the same strict oversight, inventory, and data privacy

rules as traditional school equipment. Finally, this revision protects student data and ensures human accountability while guiding the responsible use of emerging technologies. These changes are recommended but not required.

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 but not required.

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 but not required.

Policy 7540.08 - ARTIFICIAL INTELLIGENCE (AI) (Revised)

This policy provides guidance for the safe use of Artificial Intelligence (AI) in schools to support learning while also providing guiding principles for staff members.

The updates are important because they group AI into different technical categories and ban unvetted public AI tools from handling private student or staff information. These changes also protect the District by requiring strict contracts that stop outside tech companies from using school data to train their global models. Finally, the new rules add strict safeguards for autonomous AI Agents and require that any AI-generated files properly comply with public records laws. These changes are recommended but not required.

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 but not required.

Policy 8315 - PRESERVATION OF RECORDS AND LITIGATION HOLDS (Revised)

This policy is relevant because it establishes the legal framework for identifying, preserving, and protecting documents and electronically stored information when litigation is threatened or commenced against the District.

This update expands the scope of preserved data to include artificial intelligence information. It also formalizes operational protocols by requiring coordination with insurance defense counsel, the immediate suspension of automatic deletion schedules, and access limitations on District devices undergoing review. These changes are recommended, but not required.

Policy 8330 - STUDENT RECORDS (Revised)

This policy protects student privacy while providing parents and authorized staff access to school records.

The updates are important because they state that records created by Artificial Intelligence (AI) or shared through social media are official student records. These changes also make the school responsible for the safety and accuracy of AI-created files. Finally, a change clarifies that parents can look at files related to their child, no matter what format they are in or where they are stored, unless a specific legal exception applies. These changes are recommended but not required.

Policy 8330.01 - UNAUTHORIZED ACQUISITION OF STUDENT PERSONAL INFORMATION (Revised)

This policy requires the District to alert parents if a student's private information is inappropriately accessed.

The updates expand the data breach rules to cover leaks caused by Artificial Intelligence (AI) systems or outside technology vendors. Additionally, the changes allows the District does not waste resources sending out unnecessary warnings if a leak poses no real risk of fraud or identity theft. Finally, these updates keep the school aligned with updated Wisconsin state laws regarding data privacy. These changes are recommended but not required.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po5136

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised PERSONAL COMMUNICATION DEVICES

ADOPTED Apr 16, 2026

5136 - **PERSONAL COMMUNICATION DEVICES**

The District is aware that Personal Communication Devices (PCDs) are used by students and parents to communicate with each other. However, the use of PCDs on school grounds must be appropriately regulated to protect students, staff, and the learning environment.

~~"Personal communication devices" (~~ PCDs ~~)~~, also referred to as "wireless communication devices", as used in this policy, mean a portable wireless device that has the capability to provide voice, messaging, or other data communication between two (2) or more parties and includes all of the following:

A. cellular/mobile telephone;

B. tablet computer;

C. laptop computer;

D. gaming device;

E. smartphone;

F. e-reader;

G. smartwatch;

H. wearable technology;

I. AI Smart Glasses;

J. any other web-enabled devices of any type.

Students 4K-8: While students may possess PCDs in school, on school property, during before and after-school activities (e.g., extra curricular activities), and at school-

related functions, they must be powered completely off or put into silent mode and stored out of sight during school hours.

Students at the High School may use PCDs before and after school, during their lunch break, in between classes as long as they do not create a distraction, disruption, or otherwise interfere with the educational environment, during after-school activities (e.g., extra curricular activities), or at school-related functions. At all other times, PCDs must be powered off or silenced and stored out of sight. PCDs may only be used for instructional purposes at a teacher's discretion with administrator approval. In these situations, students without PCDs would have the option to use a school-issued device.

All PCD use must consistently adhere to the standards outlined in Policy 7540.08 – Artificial Intelligence (AI).

Students may not use PCDs on school property or at a school-sponsored activity to access and/or view Internet websites that are otherwise blocked to students at school. Student s are prohibited from unauthorized use of, or access to, the District's wired and/or wireless network.

During after-school activities, P CD ~~DC~~ 's shall be powered completely off and stored out of sight when directed by the administrator or sponsor (coach, advisor, etc.)

Except as authorized by a teacher, administrator, or IEP team, students are prohibited from using PCDs during the school day, including while off-campus on a field trip, to capture, record and/or transmit the words or sounds (i.e., audio) and/or images (i.e., pictures/video) of any student, staff member, or other person. Using a PCD to capture, record, and/or transmit audio and/or pictures/video of an individual without proper consent is considered an invasion of privacy and is not permitted. Students who violate this provision and/or use a PCD to violate the privacy rights of another person may have their PCD confiscated and held until the end of the school day, or a parent picks it up, and may be directed to delete the audio and/or picture/video file while the parent is present. If the violation involves potentially illegal activity, the confiscated PCD may be turned over to law enforcement.

PCDs, with cameras or any other recording capabilities, may not be activated or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include, but are not limited to, classrooms, gymnasiums, locker rooms, shower facilities, rest/bathrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The Superintendent and building principals are authorized to determine other specific locations and situations where use of a PCD is absolutely prohibited.

Students shall have no expectation of confidentiality with respect to their use of PCDs on school premises/property.

Students may not use a PCD in any way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed, or intimidated. See Policy 5517.01 – Bullying. In particular, students are prohibited from using PCDs to: (1) transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon any Protected Class consistent with Board Policy 2260 - Nondiscrimination and Access to Equal Educational Opportunity; and (2) engage in "sexting" - i.e., sending, receiving, sharing, viewing, or possessing pictures, text messages, e-mails or other materials of a sexual nature in electronic or any other form. Violation of these prohibitions shall result in disciplinary action. Furthermore, such actions will be reported to local law enforcement and child services as required by law.

Students are also prohibited from using a PCD to capture, record, and/or transmit test information or any other information in a manner constituting fraud, theft, cheating, or academic dishonesty. Likewise, students are prohibited from using PCDs to receive such information.

Possession of a PCD by a student at school during school hours and/or during extra-curricular activities is a privilege that may be forfeited by any student who fails to abide by the terms of this policy, or otherwise abuses this privilege.

Policy Violations

Violations of this policy may result in disciplinary action and/or confiscation of the PCD. The building principal will also refer the matter to law enforcement or child services if the violation involves an illegal activity (e.g., child pornography, sexting). Discipline will be imposed on an escalating scale ranging from a warning to an expulsion based on the number of previous violations and/or the nature of or circumstances surrounding a particular violation. If the PCD is confiscated, it will be released/returned to the student's parent after the student complies with any other disciplinary consequences that are imposed, unless the violation involves potentially illegal activity, in which case the PCD may be turned over to law enforcement.

A confiscated device will be marked in a removable manner with the student's name and held in a secure location in the building's central office until it is retrieved by the parent or turned over to law enforcement. School officials will not search or otherwise tamper with PCDs in District custody unless they reasonably suspect that the search is required to discover evidence of a violation of the law or other school rules. Any search will be conducted in accordance with Policy 5771 Search and Seizure. If multiple offenses occur, a student may lose the privilege to bring a PCD to school for a designated length of time or on a permanent basis.

Student use of PCDs in the following circumstances will not be considered a violation of this policy:

A. **Emergency or Threat:** Student use of a PCD is allowed in the event of an emergency or a perceived threat to address the safety and security of students and staff.

B. **Health Care Management:** Student use is authorized as necessary to manage or support a specific student's health care needs as approved by the District Nurse **and** as defined in the individual student health plan.

C. **Individualized Education Plans:** Student use is authorized consistent with a student's Individualized Education Program (IEP) or a plan developed under Section 504 of the federal Rehabilitation Act of 1973.

D. **Educational Purposes:** Student use is authorized by a teacher for legitimate educational purposes during instructional time as described above.

~~**( ) Duty to Report**~~

~~A. ( ) - person ( ) staff member ( ) student [END OF OPTIONS] - who discovers a student using a PCD in violation of this policy is required to report the violation to the building principal.~~

[END OF OPTIONAL SECTION]

Students Responsible for Their PCDs

Students are personally and solely responsible for the care and security of their PCDs. The District assumes no responsibility for theft, loss, or damage to, or misuse or unauthorized use of, PCDs brought onto its property.

Parents/guardians are advised that the best way to get in touch with their child during the school day is by calling the school office.

Students may use school phones to contact parents during the school day.

Annual Notice

No later than October 1 of each year, the Department of Public Instruction (DPI) shall be notified by the District of whether any changes have been made to this policy and, if so, the updated policy shall be submitted to the DPI.

© Neola 20 26 ~~25~~

Legal
118.13, Wis. Stats.
118.258, Wis. Stats.

120.12(29), Wis. Stats.
175.22, Wis. Stats.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po5505

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised ACADEMIC HONESTY

ADOPTED Oct 23, 2023 · REVISED Apr 13, 2026

5505 – **ACADEMIC HONESTY**

The District values honesty and expects integrity in the District's students. Violating academic honesty expectations erodes the trust between teachers and students as well as compromises the academic standing of other students. So that each student learns the skills being taught, and is judged solely on their own merits, the District prohibits any student from presenting someone else's work as their own, using artificial intelligence platforms in place of one's own work, providing unauthorized assistance to another student, and cheating in any manner.

All school work submitted for the purpose of meeting course requirements must be the individual student's original work or the original work of a group of students for group projects. It is prohibited for any student to unfairly advance their own academic performance or that of any other student. Likewise, no student may intentionally limit or impede the academic performance or intellectual pursuits of other students.

Academic dishonesty includes, but is not limited to:

A. plagiarism (of ideas, work, research, speech, art, music, etc.);

B. forgery of another's work;

C. presenting the results that are the product of an artificial intelligence (AI) platform as one's own where the use of AI was not specifically allowed by the teacher as part of the assignment;

D. downloading or copying information from other sources and presenting it as one's own;

E. using language translation work of someone else or using technology when the expectation is doing one's own translation;

F. copying another person's work;

G. allowing another person to copy one's own work;

H. stealing another person's work;

I. doing another person's work for them;

J. distributing copies of one's work for use by others;

K. distributing copies of someone else's work for use by others for academic gain or advantage;

L. intentionally accessing another's work for the purpose of presenting it as one's own for academic gain or advantage;

M. distributing or receiving answers to assignments, quizzes, tests, assessments, etc.;

N. distributing or receiving questions from quizzes, tests, assessments, etc.

O. using AI to modify another person's work to avoid detection;

P. collaborating on an assignment when independent work is required;

Q. fabricating data, citations, sources, research results, or evidence;

R. receiving unauthorized assistance from another person (tutor, parent, peer, online forum, contract service, etc.);

Use of Artificial Intelligence/Natural Language Processing Tools For 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, the use of Artificial Intelligence (AI) and Natural Language Processing (NLP) tools (collectively, "AI/NLP tools") is strictly prohibited for the completion of school work. The use of AI/NLP tools, without the express permission/consent of a teacher, undermines the learning and problem-solving skills that are essential to academic success and that the staff is tasked to develop in each student. Students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI/NLP tools and they should ask their teachers when they have questions and/or need assistance. Unauthorized use of AI/NLP tools is considered a form of plagiarism and any student found using these tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code of Conduct.

Notwithstanding the preceding, students can 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. Proper citation when using AI/NLP tools is required when non-original AI/NLP generated content is incorporated into any work product. X ~~(-)~~ Citation when using AI/NLP tools for spell check, grammar assistance, and similar refinement/editing tools does not need to be disclosed unless required by a student's teacher. ~~[END OPTION]~~ -

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 understand spoken language.

Staff and Administration have the responsibility for monitoring students' work for compliance with this policy.

When enrolled in Advanced Placement (AP), Early College Credit Programs (ECCP), Start College Now (SCN), or any other third-party, District-sponsored programming, students are expected to follow the corresponding policies and guidelines regarding the use of AI/NLP.

All teachers, beginning in the elementary grades, will educate students as to what constitutes academic dishonesty and what is acceptable and unacceptable behavior in District schools regarding academic integrity.

AI Detection Tools - AI detection tools are only preliminary investigative resources, and their findings are not conclusive proof of academic misconduct. Disciplinary action requires a comprehensive review of all evidence and established procedures, and cannot be based solely on an automated detection report.

~~()~~ Requirements for AI Detection:

1. **Not a Sole Indicator:** The use of AI detection as the sole basis for academic integrity determinations is prohibited. It should serve only as a starting point or one input in a broader inquiry.

2. ~~Employees must disclose the use of AI detection software in course syllabi, curricula, or specific assignment guidelines where it will be employed.~~ ~~Transparency:~~

3. ~~Record the specific detection result and the tool used.~~ ~~Documentation:~~

4. **Student Dialogue:** Provide the student with a formal opportunity to respond to the concern.

5. **Holistic Review:** Apply professional judgment alongside the detection output to determine if a policy violation has occurred.

~~**[END OF OPTIONAL SECTION]**~~

Before any disciplinary action is taken based in part on AI detection output, employees must exercise professional judgment rather than treating detection software results as conclusive.

Students who are found to have violated ~~violate~~ this policy are subject to disciplinary consequences.

Teachers are authorized, in consultation with their Principal, to apply appropriate consequences for violations of this policy. Disciplinary consequences for significant violations may include removal from the class with a failing grade, removal from student leadership positions, elimination of honors recognition, loss of membership in honor organizations, as well as other disciplinary consequences appropriate to the nature of the violation.

Parents/guardians shall be contacted as soon as practicable to report any alleged acts of academic dishonesty by their child.

Repeated violations of this policy at the high school level will result in additional disciplinary consequences, up to and including suspension and expulsion.

Student and/or parent/guardian appeals of disciplinary consequences resulting from violation of this policy may be made within five (5) business days to the Principal whose decision shall be final. If the Principal was the staff member responsible for the disciplinary consequence being appealed, then student and/or parent/guardian appeals should be directed within five (5) business days to the Superintendent whose decision shall be final.

A summary of this policy shall be included in the Student Handbook.

Revised 7/1/24
Revised 1/27/25
Revised 10/27/25
T.C. 4/13/26

© Neola 20 26 ~~25~~

Legal
118.01, 118.164, 120.12, Wis. Stats.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po7440.02

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised SMART SENSOR AND MONITORING TECHNOLOGY

ADOPTED Oct 27, 2025

7440.02 - **SMART MONITORING EQUIPMENT**

In order to protect students and faculty, promote security and protect the health, welfare and safety of students, staff and visitors, the Board authorizes the use of smart sensor and electronic monitoring equipment on school property, and in school buildings and school buses. Smart sensor and monitoring technology uses devices that can sense, collect, and process a variety of environmental information. Smart sensor and monitoring technology also includes utilizing Artificial Intelligence (AI) to monitor, analyze, and identify real-time and recorded video footage for surveillance and investigative purposes. Information obtained through smart sensor devices may be used to identify intruders and persons breaking the law, Board policy, or the Student Code of Conduct ~~(i.e., it may be used as evidence in disciplinary actions and criminal proceedings)~~.

The monitoring of actions and behavior of individuals who come onto school property is a significant factor in maintaining order and discipline and protecting students, staff, visitors, and school and student property. Smart sensor monitoring systems serve to complement other means being employed in the District to promote and foster a safe and secure teaching and learning environment for students and staff. The District recognizes that the use of a smart sensor monitoring system does not replace the need for the ongoing vigilance of the school staff assigned by the building principal to monitor and supervise the school building. Rather, the smart sensor monitoring system serves as an appropriate and useful tool with which to augment or support the in-person supervision provided by staff. The building principal is responsible for verifying that due diligence is observed in maintaining general campus safety and security.

The Superintendent is responsible for determining where to install and operate ~~(~~) fixed-location ~~[END OF OPTION]~~ smart sensor monitoring equipment in the District. The determination of where and when to use smart sensor equipment shall ~~will~~ be made in a nondiscriminatory manner. Smart sensor equipment may be placed in designated areas in school buildings (e.g., school hallways, restrooms, classrooms, locker rooms, entryways, the front office where students, employees, and visitors are permitted to freely come and go, gymnasiums, cafeterias, libraries).

Any person who takes action to block, move, or alter the location of a smart sensor shall be subject to disciplinary action.

Except for instructional use of smart sensor monitoring authorized by the Superintendent, any ~~Any~~ information obtained from smart sensor monitoring systems may only be used to support the orderly operation of the District's schools and facilities, and for law enforcement purposes, and not for any other purposes. As such, information obtained through the use of smart sensor equipment may be used as evidence in any disciplinary proceedings, administrative proceedings or criminal proceedings, subject to Board policy and administrative guidelines.

Smart sensor technology is to be implemented in accordance with this policy and the related guidelines. The District will not accept or tolerate the improper use of smart sensor equipment and will take appropriate action in any cases of wrongful use of this policy.

© Neola 20 26 ~~24~~

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po7540

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised TECHNOLOGY

ADOPTED Jul 1, 2019 · REVISED Oct 27, 2025

7540 - **TECHNOLOGY**

The District is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of District operations.

Students' use of District technology resources (see definition in Bylaw 0100 - Definitions) is a privilege, not a right. Students and their parents must comply with Policy 7540.03- Student Technology Acceptable Use and Safety.

This policy, along with the Student and Staff Technology Acceptable/Responsible Use policies, and the Student Code of Conduct, further govern students' and staff members' use of their personal communication devices (see Policy 7540.03- Student Technology Acceptable Use and Safety and Policy 7530.02 - Staff and School Officials Use of Personal Communication Devices). Users have no right or expectation of privacy when using District technology resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network, District-owned devices, and/or Internet connection).

Further, safeguards shall be established so that the Board's investment in both hardware and software achieves the benefits of technology and inhibits negative side effects. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, using social media, which is defined in Bylaw 0100 - Definitions, to interact with others online; interacting with other individuals online; and, recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses if they experience cyberbullying. Social media does not include sending or receiving e-mail through the use of District-issued e-mail accounts.

District Policy on Artificial Intelligence (AI) Use

The District considers Artificial Intelligence (AI) tools to be a fundamental part of its technology infrastructure. Therefore, all AI technology , including software and hardware that is procured, developed, or utilized , is subject to the same oversight, inventory, and management standards as all other District technology assets.

The Board has established Policy 7540.08 - Artificial Intelligence (AI) to ensure the ethical, responsible, and compliant use of AI by everyone in the school community.

Equipment Security and Retention Procedures

The District invests significant resources in making current technology available for staff and students. Individual usage of devices that are not in a fixed location must be in accordance with these guidelines. The term "device" for purposes of this guideline includes District-owned computers, tablets, smart devices, and any other hardware or software systems or equipment owned or leased by the District.

A. **Identification:**

1. A label with the District's name and an identification number will be placed on each device owned by the District.

2. Records of the identification number, serial number, model, etc. for each device shall be maintained in the Technology Department.

3. Records on each piece of software and software license, organized by title and course or program, shall be maintained in the Technology Department.

4. District devices are assigned, identified, and tracked through an online management system.

B. **Use of District-owned Devices:**

All devices to be used either in the District or off-school premises shall be checked out through the Building LMCs or Technology Deptartment. Devices may not be used for the purpose of copying materials in violation of copyright laws.

No device may be used to access any material that is prohibited by the District's technology usage policies, Policy 7540.03 - Student Technology Acceptable Use and Safety and Policy 7540.04 - Staff Technology Acceptable Use and Safety. Devices may not be used to access content that is unlawful or potentially harmful to the device and may never be used to access any "darkweb" content. Specifically, use of devices to access material that poses a risk of introducing viruses, malware, or other destructive content is strictly prohibited. Users are responsible for replacing devices that are inoperable due to the introduction of such malicious content while in the user's possession.

C. **Requests for Personal Use:**

Personal use of devices by students, staff, and shall be in accordance with Policy 7530 - Lending of District-Owned Equipment.

Additionally, a device shall not be used to access any material that is prohibited by the District's technology usage policies. (See Policy 7540.03 - Student Technology Acceptable Use and Safety and Policy 7540.04 - Staff Technology Acceptable Use and Safety)

If allowed for personal use, devices may not be used to access content that is unlawful or potentially harmful to the device and may never be used to access any "darkweb" content. Specifically, use of devices to access material that poses a risk of introducing viruses, malware, or other destructive content is strictly prohibited. Users are responsible for replacing devices that are inoperable due to the introduction of such malicious content while in the user's possession.

No business use shall be made of any borrowed devices. Software shall not be used in violation of any licensing agreement, nor shall it be copied.

No software or other applications may be downloaded onto any device except by the District's Technology Department and only as authorized by the District Administrator.

Users will be responsible for arranging safe transportation and housing for use off school premises.

D. **Staff Services:**

Media staff will instruct the user on the correct operation of devices. Media staff may assist other staff members in obtaining materials for instructional use by recording and/or copying within copyright guidelines.

E. **Equipment Inventory and Repair:**

All devices will be inventoried pursuant to Policy 7450 - Property Inventory.

If a piece of equipment requires repair, it will be sent to the contracted and licensed repair company for the equipment.

F. **Report of Loss:**

If any device is lost, the Principal and the Technology Director shall be notified. The Principal may notify the police if deemed appropriate.

Access to Social Media

Staff use of District-approved social media platforms/sites shall be consistent with Policy 7544 - Use of Social Media.

Students must comply with Policy 7540.03 - Student Technology Acceptable Use and Safety and Policy 5136 - Personal Communication Devices when using District technology resources to access and/or use District-approved social media platforms/sites. Similarly, staff must comply with Policy 7544 - Use of Social Media, Policy 7540.04 - Staff Technology Acceptable Use and Safety, and Policy 7530.02 - Staff and School Officials Use of Personal Communication Devices when using District technology resources to access and/or use District-approved social media platforms/sites.

Revised 4/12/21
Revised 5/22/23
Revised 10/27/25
Revised 5/13/24

© Neola 20 26 ~~23~~

Legal
947.0125, Wis. Stats.
948.11, Wis. Stats.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po7540.03

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

ADOPTED Jul 1, 2019 · REVISED Jun 8, 2026

7540.03 - **STUDENT TECHNOLOGY RESPONSIBLE USE AND SAFETY**

The District understands the importance of teachers, students and families engaging, collaborating, learning, and sharing in digital environments. The District is committed to developing and providing technology resources that promote learning to facilitate resource sharing, content creation, collaboration, innovation, and communication.

Technology use, whether the technology is owned by the District or the user, involves personal responsibility.

For the purposes of this policy, electronic information, network resources, and communication services include, but are not limited to: network services (both wired and wireless), hardware, mobile devices, software, social media tools, learning management systems, web-based tools, telecommunications services, email services, and audio/video equipment.

The District's computer network and Internet system do not serve as a public access service or a public forum, and the District imposes reasonable restrictions on its use consistent with its limited educational purpose.

Guiding Principles for Students:

A. Communicating: Although you are personally responsible for work you publish online, including social media sites, using a District account means that you represent DASD. Your online behavior should reflect the same District standards of equity, honesty, respect, and consideration that are expected in face-to-face communication.

B. Representing Yourself: When selecting images, signatures, and other similar elements for social media and communication, consider all audiences, purpose, and copyright laws.

C. Privacy: Your privacy has two parts. First, use of the district's networks (wired or wireless) and communication resources should not be considered private. Network activity is monitored, logged, and reported regularly as part of Learning Information Systems operations and security. Second, keeping your personal information private is a student's responsibility. This responsibility includes keeping accounts and passwords secure.

D. Your Devices: DASD will provide students with devices to use for educational purposes. These devices might be stored at the school or brought back and forth each day, depending on the grade level. Students may use personal devices at school, but it's up to the teacher and administrators when, where and how that might be. Appropriate use rules and disciplinary policies apply no matter which device is in use. For some events, like statewide testing, a school-issued device may be required.

E. Collaboration: What you do online should not be different than the way you would behave face-to-face. Students will be asked to follow the District's Videoconferencing Guidelines.

F. Personal Responsibility: Students have personal responsibility for devices and for District-issued accounts. Accounts and associated passwords should be kept secure and private. Devices, whether it is your school-issued device or your own, or you bring a personal device to school, is your responsibility to keep safe throughout the day. If your device won't be with you, plan for where you can keep it secure. If your device is damaged or not working as needed, students or families should use District-approved methods for accessing help and/or repair.

G. Digital Citizen: Being a positive digital citizen means that students are managing their digital identity and behaving in ways that support safe, legal, and ethical practices, includes online behavior, but also including respecting the work of others by following copyright and intellectual property laws.

The District regulates the use of District technology resources by principles 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 the Student Code of Conduct govern students' use of District Technology Resources (including District-issued accounts) and students' personal communication devices when they are connected to the District computer network (including wireless), Internet connection, and/or online educational services/apps managed by the District, or when used while the student is on District-owned property or at a District-sponsored activity (see Policy 5136).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and similar).

Because its Technology Resources are not unlimited, the District has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printing.

Users have no right or expectation to privacy when using District Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network, wireless access, mobile hotspots, and/or Internet connection).

First, the District may not be able to technologically limit access to services through its technology resources to only those that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity 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), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the District 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. At the discretion of the Superintendent or designee, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measures may not be disabled at any time that students may be using the District technology resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The District utilizes software and/or hardware to monitor online activity of students and to block/filter access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254(h)(7)) as any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

B. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;

C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

At the discretion of the Superintendent or designee, the technology protection measure may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measure may not be disabled at any time that students may be using the District technology resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act (CIPA). Any student who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or Learning Information Systems Coordinator 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 measure. 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 measure.

The Superintendent or Learning Information Systems Coordinator may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

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

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", "harvesting", digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students online;

D. unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors.

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while at school, virtually, or in-person.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools.

The District expects that staff members will provide guidance and instruction to students in the appropriate use of District technology. Such training shall include, but not be limited to, education concerning digital citizenship, positive collaboration and communication, appropriate online behavior, and cyberbullying awareness and response. All users of District technology resources (and their parents/guardians if they are minors) are required to acknowledge this responsibility during the annual student registration process to abide by the terms and conditions of this policy and its accompanying guidelines. An age-appropriate version of this policy will be provided for younger students.

Off premises use of E-Rate supported technology must be primarily for an educational purpose that is integral, immediate, and proximate to the education of students.

Students will be assigned a school email account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and 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 email account when signing up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes and meet the appropriate terms of service and privacy policies for student use.

Students are responsible for responsible behavior when using District technology resources - i.e., behavior comparable to that expected of students when they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. The District does not approve any use of its technology resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

District-Approved PCD Communication Platforms - The Superintendent is required to designate and communicate the District-approved social media/communication platforms/sites which all Board members, staff, coaches/advisors, and approved volunteers are required to use exclusively when communicating with each other and/or with students.

The approved communication platform(s) is/are:

A. District email and Google Workspace for Education;

B. ParentSquare and StudentSquare (Grades 7-12);

C. District-approved social media accounts.

The District has also approved the use of athletic and extra-curricular management tools Bound and Hudl for narrow, functional purposes such as physicals, forms, game tickets, livestreaming, film study, student-athlete profiles. These tools are not approved communication platforms for direct messaging.

When students communicate with staff, volunteers, or Board members using PCDs, discussions must be appropriate, professional, and related to legitimate school purposes. These communications shall occur only when absolutely necessary. Appropriate content includes:

A. Instructional communication (assignments, coursework, academic support);

B. School-related activities (clubs, athletics, events, field trips, rehearsals);

C. Scheduling or logistical information related to classes or school programs;

D. Pedagogical assistance related to school participation (clarifying expectations, reminders, or academic assistance); and,

E. Safety or emergency communication when necessary.

Communications must remain professional in tone, limited to educational or school-related matters, and consistent with District policies regarding staff–student boundaries. Failure to follow these policy expectations may result in discipline up to and including termination, as well as referral to law enforcement if deemed appropriate. The level of discipline will depend on the severity of the violation. This policy applies to communication that occurs during or outside of school hours.

Authorized and Appropriate Use of Artificial Intelligence (AI)

All use of AI technology by students must adhere to the requirements and standards detailed in Policy 7540.08 – 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 of a nude or partially nude person, or of a person engaged in sexual activity, or as otherwise prohibited by law that is 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.

~~**Expectations for Responsible Artificial Intelligence (AI) Use**~~ **AI Prohibited Data Input**

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, 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 Codes of Conduct and other applicable Board policies.

Academic Honesty

The unauthorized use of Artificial Intelligence tools to generate or complete academic work shall constitute a violation of the District's policy on academic honesty. (See Policy 5505 - Academic Honesty)

All student use of AI technology must comply with the requirements and standards set forth in Policy 7540.08 – 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 technology resources that are not authorized by this policy and its accompanying guidelines.

The District designates the Superintendent and Learning Information Systems Coordinator as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District technology resources.

Revised 4/12/21
Revised 7/24
Revised 6/9/25

© Neola 2026

Legal

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246
47 C.F.R. 54.500 - 54.509, 54.511, 54.513 - 54.520, 54.522 - 54.523
942.09, Wis. Stats.
118.07(7), Wis. Stats.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po7540.08

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised ARTIFICIAL INTELLIGENCE (AI)

ADOPTED Oct 23, 2023 · REVISED Apr 16, 2026

7540.08 - **ARTIFICIAL INTELLIGENCE (AI)**

The District acknowledges the positive impact and transformative potential of Artificial Intelligence (AI) in education and operations, emphasizing a balanced, people-centered approach. It supports the responsible and innovative use of AI in classrooms and professional settings, with the understanding that AI should enhance human interaction and instruction, not replace it, and all AI-driven decisions require human review. The Superintendent is authorized to support the use of artificial intelligence technology when its use is consistent with the District's mission, goals, and operational integrity.
The Superintendent is responsible for overseeing and ensuring compliance of this policy.

Definitions

For purposes of this policy, the following definitions apply:

Artificial Intelligence (AI)

AI refers to systems or tools capable of performing tasks that typically require human intelligence including, but not limited to, decision-making, problem-solving, and language understanding. AI is computer code that can resemble human intelligence to complete a given task (e.g., problem-solving, planning, etc.). It involves developing algorithms and systems that can perceive, reason, learn, and make decisions based on data made available to the AI tool.

Generative AI

A subset of AI that uses large language models (LLMs) and other advanced algorithms to create content, such as text, images, audio, or video, in response to user input.

Generative AI works by analyzing large datasets to learn patterns and features, which it then uses to generate new, original content. It uses complex algorithms, often based on neural networks, to make predictions based on the input data it has processed; thereby enabling it to create a wide range of outputs, from text and images to music and code, that mimic the style or characteristics of the data on which it was trained.

At its core, generative AI predicts the flows of language. Trained on massive amounts of text taken from publicly available internet sources to recognize the relationships that most commonly exist between individual units of meaning (including full or partial words, phrases, and sentences), LLMs can, with great frequency, generate replies to users' prompts that are contextually appropriate, linguistically facile, and factually correct.

Natural Language Processing (NLP)

A field of artificial intelligence that focuses on enabling computers to understand, interpret, and respond to human language in a meaningful way. Examples of NLP include, but are not limited to, Grammarly, GPT-Based APIs, Google Cloud Natural Language AI, Microsoft Azure Text Analytics, IBM Watson NLP, Amazon Comprehend, etc.

Large Language Model (LLM)

A sophisticated AI system trained on extensive text data to process and produce language; recognize patterns, grammar, and nuances. It can perform tasks like text generation, question answering, and language translation.

Algorithm

A set of rules or instructions guiding AI operations and decision-making.

Personally Identifiable Data/Personal Data

Refers to any information that can directly or indirectly identify an individual including, but not limited to, names, addresses, student records, and health information.

Proprietary Information/Data

Refers to a broad category of non-public, sensitive, or confidential data belonging to the District, its staff, or its operations. This information is considered the District's. This information is generally protected from unauthorized disclosure or use.

Public-Domain AI

AI models where the developers may openly share the model's architecture (Open-Source) or provide free, public access to a closed-source interface (e.g., standard web-based chatbots). Because these tools are typically used without a formal District contract, they present a high risk of data exposure.

1. **Shared Data Training:** Data input into these tools is frequently used to train the global model, making the information publicly available or accessible to the provider.

2. **Lack of Filtering:** These models may require the District to manually implement its own "wrapper" or filtering layers to manage safety.

3. **Reliability Issues:** Content produced may be less reliable as it often draws from unverified, publicly scraped data sources.

Due to the high potential for violating Federal and State privacy laws (including FERPA and 118.125, Wis. Stat s .), the use of Public-Domain AI is prohibited for any task involving student records, Personally Identifiable Information(PII) , or confidential District operations.

~~**Open AI ("Open-Source AI")**~~

~~Definition: AI models where the developers openly share the model's architecture, underlying code, and often the "weights" (the learned parameters of the model), and sometimes the training data. Open AI models accessed publicly present a high risk of data release, as data input is often used for AI tool training and can be publicly available. Open AI models may require the District to implement and manage its own wrapper or filtering layer. As a result, it is not recommended that Open AI tools/applications are used in districts due to the high potential of violating Federal and State laws. Open-Source AI also produces less reliable content, because it is accessing a pool of data that is not universally verified as accurate.~~

~~**Closed AI ("Closed-Source/Proprietary AI")**~~

~~Definition: AI models where the developers obscure or protect the model's architecture, underlying code, training data, and weights. Users interact with the model via a restricted service. Closed AI may offer better, contractually-guaranteed data security (e.g., "enterprise" versions), but its "black box" nature still requires a formal audit and contract. Closed AI developers typically manage these filters internally. Closed-Source or Proprietary AI produces more reliable results because it is accessing data sources that are controlled and can be verified as accurate.~~

~~Any use of artificial intelligence technology in the District's educational program or operations must be in accordance with State and Federal law as well as Board policies~~ ~~**( )**~~ ~~including, but not limited to, the following: Policy 5505 – Academic Honesty; Policy 5500 – Student Code of Classroom Conduct; Policy 5500.01 – Conduct in Virtual Classroom; Policy 5517 – Student Anti-Harassment; Policy 5517.01 – Bullying; Policy 2266 – Nondiscrimination on the Basis of Sex in Education Programs and Activities; Policy 8330 – Student Records; Policy 2240 – Controversial Issues in the Classroom; Policy 7540.03 – Student Technology Acceptable Use and Safety; and Policy 7540.04 – Staff Technology Acceptable Use and Safety.~~ ~~**[DRAFTING NOTE: Confirm and Select as Needed] [END OF OPTION]**~~

Enterprise-Grade AI

AI models where the developers protect the model's architecture, underlying code, and training data, typically providing access via a restricted service or "black box" interface. Unlike consumer tools, Enterprise-Grade AI is provided under a formal contract or agreement that:

1. **Guarantees Data Privacy & Security:** Ensures all District data remains isolated within a private "tenant" or environment.

2. **Prohibits Model Training:** Strictly ensures that District data, including student and staff information, is not used to train the provider's global models.

3. **Provides Managed Oversight:** Includes internally managed filters and verifiable data sources, often producing more reliable and accurate results than unvetted models.

Due to the "black box" nature of these systems, the District still requires a formal audit and contract to verify that these security and privacy safeguards are technically enforced.

Locally Hosted AI

AI models deployed and operated entirely on District-owned hardware, with no data transmitted to external servers. Locally hosted models may be either consumer-grade or enterprise-grade in origin. When properly configured, locally hosted AI tools represent a high standard of data privacy because student and staff data never leaves District infrastructure. The District still requires a formal audit to verify that these security and privacy safeguards are technically enforced.

AI Agent

An AI agent is an autonomous software entity that can observe its environment, make decisions, and take actions to achieve specific goals without direct human intervention for every step. Unlike standard AI chatbots, AI Agents have the capacity to execute tasks (e.g., sending emails, modifying files). Due to the heightened risks regarding network security, data confidentiality, and the potential for autonomous errors, the use of AI Agents requires a higher level of review and **(X)** ~~written~~ **[END OF OPTION]** a pproval from the **(X)** Superintendent or Learning and Information Systems Coordinator (LIS) ~~IT Department~~ **(X)** _____ **[END OF OPTIONS]** prior to implementation.

General Principles

A. **Transparency**

Users of AI tools must disclose when and how these tools have been employed in the creation of academic work, ~~or~~ professional work, or used to influence and/or make decisions. (X) Spell check, grammar assistance, and similar refinement/editing tools do not need to be disclosed unless required by a student's teacher.

B. **Ethical Use**

District employees who use AI technologies must do so in ways consistent with institutional values, privacy standards, Family Educational Rights and Privacy Act (FERPA), Individual with Disabilities Education Act (IDEA), copyright laws, and ethical principles, honesty, trustworthiness, and personal dignity of both employees and students.

C. **Content Responsibility**

District employees who use AI technologies are responsible for the content created by that AI tool.

D. **Use of AI in Relation to Other Policies**

Any use of artificial intelligence technology in the District's educational program or operations must be in accordance with State and Federal law as well as Board policies including, but not limited to, the following: Policy 5505 – Academic Honesty; Policy 5500 – Student Code of Classroom Conduct; Policy 5500.01 – Conduct in Virtual Classroom; Policy 5517 – Student Anti-Harassment; Policy 5517.01 – Bullying; Policy 2266 – Nondiscrimination on the Basis of Sex in Education Programs and Activities; Policy 2240 – Controversial Issues in the Classroom; Policy 8310 - Public Records; Policy 8330 – Student Records; Policy 7540.03 – Student Technology Acceptable Use and Safety; and Policy 7540.04 – Staff Technology Acceptable Use and Safety.

AI Tool ~~**Evaluation and**~~ **Approval**

[DRAFTING NOTE: Choose one, two, or three of the options below. The district should understand all legal risks associated with this selection.]

The District will approve the use of ~~Public-Domain AI~~ **(** ~~( )~~ X **)** Enterprise-Grade AI, **(** X **)** Locally Hosted AI tool(s) **[** END OF OPTIONS **]** once each tool has been reviewed and verified for compliance with Federal law, State statute, and Board policies.

[END OF OPTIONS]

AI Tool Evaluation

Before adopting any AI tool or system, the District will conduct a comprehensive risk assessment — evaluating data sources (including use of student Personally Identifiable Information), decision-making impacts on students, potential bias or disparate impact, and vendor compliance with privacy, security, and data retention laws — and ensure all contracts include clear legal, ethical, and technical safeguards aligned with FERPA, IDEA, COPPA, PPRA, Wisconsin statutes, and District policies. AI systems must be reviewed to ensure they are nondiscriminatory, fully accessible, and do not compromise the rights or individualized support of students, particularly those protected under federal and state civil rights laws.

AI Tool Selection

The District approves the use of ~~Closed~~ AI tools as delineated in the policy ~~only~~, that have been carefully reviewed, evaluated and approved by the Superintendent for students and staff use.

Transparency

The District is committed to transparency and accountability in AI use by informing teachers, students, and parents when AI influences or makes decisions, clearly explaining how it works and what data it uses, assigning oversight to administrative staff, and conducting regular audits to evaluate accuracy, fairness, and impact on equity and student rights. [X] The District will maintain a public AI Tool Inventory that lists every approved AI tool and includes a summary of its data-handling and privacy features.

Vendor Vetting & Contracts

All AI tools used by the District must undergo a formal risk assessment by the Learning and Information Systems ~~IT/Legal~~ department to review their Terms of Service and data handling practices to ensure compliance with all Federal and State privacy laws.The District prohibits the input by any user of any student information, staff information, or confidential district data into any AI tool that does not have a formal, vetted contract guaranteeing data privacy and non-use for training.

[DRAFTING NOTE : It is recommended that the District maintain a list for clarity, but one is not required.]

(X) The District maintains a centralized Approved AI Tool Inventory. Any tool not identified on this list is considered legally unvetted and is prohibited for District use. [END OF OPTIONS]

Compliance with Student Data Privacy Mandates

All contracts with third-party AI providers that involve the processing, storage, or transmission of student data must include a formal Data Protection Addendum (DPA). To ensure compliance with all federal laws, state statutes, and district policies (including but not limited to FERPA (34 CFR 99.31) and 118.125, Wis. Stat s .), the DPA must technically and legally enforce the following:

1. **School Official Designation:** The Vendor must contractually acknowledge that it is acting as a "School Official" with a legitimate educational interest. The Vendor shall remain under the "direct control" of the District regarding the use and maintenance of all education records.

2. **Data Ownership & Custody:** The District retains sole ownership and legal custody of all data provided to or generated by the AI tool. The Vendor is prohibited from claiming any proprietary interest in student-generated content or District-provided PII.

3. **Prohibition on Model Training:** The Vendor must provide a "Zero-Retention" or "Private Tenant" guarantee, ensuring that District data—including de-identified or "anonymized" inputs—is never used to train, refine, or improve the Vendor's global AI models or shared with third-party aggregators.

4. **Security & Breach Notification:** The Vendor must employ industry-standard encryption (AES-256 or higher) and provide immediate notification within ____ (X) 72 ~~- [INSERT NUMBER]~~ hours of any suspected unauthorized acquisition of student personal information, in alignment with Policy 8330.01 - Unauthorized Acquisition of Student Personal Information. **[~~DRAFTING NOTE : Since the State legal requirement is 45 days, many districts use their contracts to create a much tighter window (often 24, 48, or 72 hours) to allow enough time to investigate before the 45-day clock runs out - 134.94, Wis. Stat s .]~~**

5. **Right to Audit & Deletion:** The District reserves the right to audit the Vendor's data-handling logs. Upon termination of the agreement, the Vendor must provide a certificate of destruction for all District data as soon as commercially practicable. ~~within thirty (30) days.~~

Employee Use of AI

1. **Instructional Integration:** Employees may integrate AI tools into their instruction at their discretion and should clearly define the parameters for AI usage in the classroom by students using only District-approved AI applications/tools.

2. **Transparency & Professional Responsibility:** When using AI to create instructional materials, assessments, or feedback, employees shall maintain transparency by disclosing the role of AI in these processes. Employees must review

and verify the accuracy and appropriateness of any AI-generated content. While AI may be used to assist with routine support functions, employees remain responsible for the intellectual core and final verification of all professional work products (including lesson plans, evaluations, and communications) to ensure the accuracy and appropriateness of the content.

3. **Data Privacy & Information Security:** Employees shall not input sensitive, confidential, personally identifiable, or proprietary information about students, colleagues, or institutional operations into AI systems that lack safeguards and policies to protect such data from being used in their training models. ~~, and if such information will be entered into an AI system, employees shall seek the approval of their ( ) supervisor ( ) Principal [END OF OPTION] before doing so.~~ **(X)** If an employee intends to enter personally identifiable information, sensitive or proprietary data into an AI tool, they must first ensure the tool is on the District's Approved AI Tool Inventory. If it is not, they must seek ~~written~~ approval from their **(** X **)** Principal **(** X **)** Director of Instructional Services and/or Director of Student Services ~~Supervisor~~ **[END OF OPTION S]**, who will consult with the **(** X **)** Learning and Information Systems Department ~~IT Department _____ [END OF OPTIONS]~~ regarding legal and privacy safeguards. ~~( )~~

4. **Academic Integrity & Detection:** Using AI detection software to enforce academic integrity should be done in accordance with the knowledge that this software is not foolproof and that the disruptive nature of AI technologies in education can lead to considerable confusion regarding expectations for AI use. Employees should use AI-detection ethically and as the starting point of an inquiry into a possible violation of academic integrity rather than as a definitive indication of student dishonesty. Employees must also disclose the use of AI software in course curricula.

5. **Workflow Enhancement:** Employees may use AI tools to enhance workflows, such as drafting communications, analyzing data, or developing reports, provided the outputs are verified for accuracy and compliance with State and Board policies. The use of AI tools for such purposes should be disclosed when disseminating AI output.

6. **Records Management:** Any record, or portion thereof, generated or compiled by an artificial intelligence (AI) system is subject to all provisions of this policy, other applicable Board policies, **(** X - **)** administrative guidelines , **[END OPTION]** and state or federal laws. The District is fully responsible for the accuracy, security, access, and disclosure of all AI-generated content within a record, as if created solely by a District employee. (see policy 8330 - Student Records and policy 8310 - Public Records)

7. **Behavioral Prohibitions:** Staff members are prohibited from using artificial intelligence (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.

Student Use of AI

1. **Instruction:** Students shall receive age appropriate instruction about responsible AI use, digital citizenship, privacy, and the risks/limitations of AI prior to using AI.

2. **Academic Standard and Authorized Use:** Students are expected to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI tools and they should ask their teacher(s) when they have questions and/or need assistance. Students may use AI tools for academic purposes when specifically and clearly permitted by their teacher(s). The use of AI must be properly disclosed and cited in accordance with the established guidelines and not be employed to undermine authentic learning or learning objectives for the course or assignment. If a student has any questions about whether they are permitted to use AI tools for a specific class assignment, they should ask their teacher(s).

3. **Behavioral Prohibitions:** Students are prohibited from using 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 Code of Classroom Conduct and other applicable Board policies.

4. **Academic Misconduct and Consequences:** Unauthorized use of AI tools will be considered a form of plagiarism, unauthorized collaboration, or misrepresentation of AI-generated content as original work and any student found using these tools without permission or in a prohibited manner will be disciplined in accordance with the Student Handbook or Policy 5500 – Student Code of Conduct and Policy 5505 – Academic Honesty. **[DRAFTING NOTE: Confirm the Board has adopted both of these policies if included in this policy]** AI-detection results shall not serve as the sole basis for a finding of academic dishonesty without additional corroborating evidence or student inquiry.

5. **Academic Accessibility:** AI tools can be utilized to assist students with disabilities in accessing and understanding written materials. For example, text-to-speech software can help students with specific learning disabilities, visual impairments, or other disabilities in reading texts, and AI-powered translation tools can help students with hearing impairments understand spoken language (e.g., create transcripts or provide closed-captioning for spoken material). Specific use of AI

technologies beyond universal application for students with disabilities is best addressed in each student's Individual Education Plan (IEP).

6. **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.

Employee Training

Employees will receive training periodically to ensure adherence to this and other related policies, data privacy, student records, and allowable/approved AI tools in the District.

Non-Academic Use of AI

Students and staff are prohibited in the use of AI from generating false or knowingly misleading representations of other students, staff, volunteers, or Board members that are reasonably interpreted as derogatory, threatening, or otherwise objectionable to a reasonable person, including by way of AI generated or manipulated visual or verbal depictions of any such individual, or the distribution of such depictions through any means, for example via social media, regardless of whether the distributor created the depictions themselves.

Enforcement

Violation of this policy may result in disciplinary consequences. Students may be disciplined for violations, up to and including suspension or expulsion. Staff may be disciplined for violations, up to and including suspension or termination of employment. The Superintendent will refer any illegal acts to law enforcement.

Questions or Concerns

Staff, parents, or members of the public who have questions or concerns regarding this policy or the use of AI in the District should contact the Superintendent.

© Neola 20 26 ~~25~~

942.09, Wis. Stats.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po8310

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised PUBLIC RECORDS

ADOPTED Jul 1, 2019 · REVISED Feb 27, 2025

8310 - **PUBLIC RECORDS**

The District recognizes its responsibility to maintain the public records of this District and to make such records available for inspection and reproduction. The Board designates the Superintendent as the District Records Custodian (DRC), to be the legal custodian of records for the District.

The DRC shall safely keep and preserve the public records of the District and shall have the authority to render decisions and carry out duties related to those public records, including providing the notice required under 19.34(1) Wis. Stats., identifying the positions of the District that constitute a local public office pursuant to 19.32(1dm), and 19.42 (7w), Wis. Stats., and other required information. The DRC may deny access to records only in accordance with the law. The DRC is authorized and encouraged to consult with the District's legal counsel to determine whether to deny access to a records request in whole or in part.

Under the Wisconsin Public Records Law, a "record" is defined as any material on which written, drawn, printed, spoken, visual, or electromagnetic information or electronically generated or stored data is recorded or preserved, regardless of physical form or characteristics, that has been created or is being kept by the authority. It includes handwritten, typed, or printed pages, maps, charts, photographs, films, recordings, tapes, optical discs, and any other medium on which electronically generated or stored data is recorded or preserved. A "record" does not include drafts, notes, preliminary computations, and like materials prepared for the originator's personal use or prepared by the originator in the name of a person for whom the originator is working; materials that are purely the personal property of the custodian and have no relation to the office held; materials to which access is limited by copyright, patent, or bequest; and published materials in the possession of an authority other than a public library that are available for sale, or that are available for inspection at a public library. The personal use exception applies to notes created by the originator solely for the purpose of refreshing the originator's recollection and as a matter of convenience (not part of assigned job duties), but does not apply to notes that are distributed to others for the purpose of communicating information or notes that are created or retained for the purpose of memorializing agency activity.

Any record, or portion thereof, generated or compiled by an Artificial Intelligence (AI) system and/or social media/ Personal Communication Devices (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. ~~(~~

In addition, records may be exempted from disclosure as a matter of statute or common law or, under the balancing test, the public interest in disclosure may be outweighed by the public interest in non-disclosure.

Any person may make an oral or written request for any public records of the District. The person may inspect or receive copies of the public record requested. The District will respond as soon as practicable and without delay , however, the amount of time a request takes to complete varies based on the volume and complexity of the request, the volume of records located that require review, available staff time to complete the request, and other factors that affect the process of fulfilling a request . The District will either provide the requested documents, subject to any redactions, or inform the requester of the District's decision to deny the request and the reason for the denial .

The District will comply with the Safe at Home/Address Confidentiality Program administered by the Wisconsin Department of Justice. (See Policy 5111 - Eligibility of Resident/Nonresident Students, Policy 8320 - Personnel Records, and Policy 8330 - Student Records.)

The District may impose a fee upon the requester of a copy of a record, which represents the actual, necessary, and direct cost of reproduction of the record. In addition, the District may impose a fee upon a requester for the actual time spent by District employees in locating a record, if the cost is $50.00 or more. In calculating location costs, the District will use the applicable employee's hourly rate for salary and benefits.

The District may also charge the requester for any equipment required to fill the request (such as videotapes, computer disks, etc.). The District may impose a fee upon a requester for the actual, necessary, and direct cost of mailing or shipping of any copies which are mailed or shipped to the requester.

The District may require prepayment of fees if the total amount exceeds $5.00. If payment is required, the District will calculate the actual cost and charge the requester. If advance payment is required, the District will either invoice the requester for the difference between the estimate and actual cost or refund any overpayment.

~~The District may provide copies of a record without charge or at a reduced charge where the District determines that the waiver or reduction of the fee is in the public interest.~~

~~[END OF OPTION]~~ ~~[ ]~~

No 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 duties.

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

Records Retention Schedule

19.21(6), Wis. Stats. requires that school districts retain public records, other than student records, for seven (7) years, unless a shorter period is fixed by the Public Records Board (PRB) in a records retention schedule subsequently adopted by the Board.

The Board has approved the following current records retention schedules developed by the Wisconsin Historical Society and PRB: Wisconsin Public School District and Related Records GRS

The District will retain public records in accordance with the preceding general records schedule(s). In the event that the preceding general records schedules adopted do not define the retention period for a particular record, the District will retain the record for seven (7) years.

Revised 11/25/19
Revised 4/12/21
Revised 10/23/23
Revised 5/13/24
T.C. 2/27/25

© Neola 20 26 ~~24~~

Legal
19.21, Wis. Stats.
19.31-39, Wis. Stats.
19.42, Wis. Stats.
118.125, Wis. Stats.
120.13(12), Wis. Stats.

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po8315

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised PRESERVATION OF RECORDS AND LITIGATION HOLDS

ADOPTED Jul 1, 2019 · REVISED May 22, 2023

8315 - PRESERVATION OF RECORDS AND LITIGATION HOLDS ~~**INFORMATION MANAGEMENT**~~

~~The Board recognizes its responsibility, in certain circumstances, to maintain information created, maintained or otherwise stored by the District outside the "Records Retention Schedule" in Policy 8310 - Public Records. In such situations, a "Litigation Hold" procedure will be utilized to identify and preserve information relevant to a specific matter. "Information" includes both paper documents and electronically stored information ("ESI"). When implementing the "Litigation Hold," the District will identify individuals in possession or custody of paper documents, ESI and electronic media containing ESI, and inform them of their obligation to preserve the documents and ESI outside the "Records Retention Schedule" in Policy 8310. The District will also identify third parties with custody or control over paper documents, ESI, or electronic media storing ESI, and request them to preserve that information. All information falling within a "Litigation Hold," which is under the control of the District, must be preserved in a readily accessible form under the requirements of Policy 8310. Failure to comply with a Litigation Hold notice ( ) may ( ) shall result in disciplinary action, up to and including possible termination.~~

The ~~Instances where the~~ Board must preserve records and Electronically Stored Information (ESI) beyond ~~maintain information outside~~ the " Records Retention Schedule " in Policy 8310 - Public Records when ~~include~~:

A. ~~when the District has specific information and/or written notice from an individual, parent or student of an intent to file an appeal of student discipline to State court;~~

B. ~~when~~ the District receives ~~has~~ specific information and/or written notice that litigation has been commenced or when it is threatened or imminent even though the litigation has not yet been filed in any tribunal. Litigation Hold expectations apply in threatened or imminent litigation in federal or state court, before an administrative agency, or upon service of a notice of circumstances of a claim pursuant to Wis. Stats. 893.80; ~~in Federal or State court;~~

C. ~~when the District is served with litigation, including, but not limited to, notice of a lawsuit in Federal or State court, or notice of a student disciplinary appeal to State court;~~

D. ~~when the District receives specific information and/or written notification from an employee, labor union, or other person of an intent to file a claim against the Board, its members, employees, or agents at an administrative agency such as the Equal Employment Opportunity Commission, Wisconsin Employment Relations Commission, U.S. Department of Education Office for Civil Rights, or a Wisconsin Equal Rights Division regarding a claim against the Board, its members, employees or agents;~~

E. ~~when the District receives specific information and/or written notification from an administrative agency such as the Equal Employment Opportunity Commission, Wisconsin Employment Relations Commission, U.S. Department of Education Office for Civil Rights, or a Wisconsin Equal Rights Division regarding a claim against the Board, its members, employees or agents;~~

F. ~~when~~ the District receives written notification from a third party requesting that the Board maintain information that could be at issue in litigation or potential litigation against a ~~that~~ third party;

G. ~~when the District Administrator recommends the termination of an employee to the Board pursuant to a labor contract;~~

H. when the District explores, contemplates initiating, or initiates litigation.

All information falling within a Litigation Hold, which is under the control of the District, must be preserved in a readily accessible form under the requirements of Policy 8310 - Public Records. An employee's failure to comply with a Litigation Hold notice and this Policy shall subject the employee to disciplinary action, up to and including termination of employment in accordance with Policy 3139-4139 - Staff Discipline ~~and the Employee Handbook~~ ~~[END OF OPTION]~~ . \ ~~(~~)

Any board member or District employee who receives specific information or written notice that may trigger a Litigation Hold shall immediately provide that information or notice to the District Administrator.

When implementing a Litigation Hold, the District Administrator shall notify the District's insurance company or broker, when appropriate, and follow the direction of appointed insurance defense counsel. The District shall take reasonable steps, with the help of the insurance defense counsel, to determine the scope of the hold, including identifying individuals who have relevant information, identifying where relevant records and ESI are stored, and preserving such materials. The District Administrator shall notify individuals in possession or custody of records and ESI, and inform them of their obligation to preserve

records and ESI outside the Records Retention Schedule in Policy 8310 - Public Records. The District shall suspend routine destruction, deletion, overwriting, or automatic retention rules for records and ESI covered by the hold.

If a staff member's or board member's District-provided device (computer, cell phone, etc.) must be taken out of service to properly preserve the contents due to a Litigation Hold, that individual may not access the device for any reason, including for access to personal items that may have been stored. Once a device is placed on a Litigation Hold, access will be limited to those authorized to access the device pursuant to the advice of legal counsel in consultation with IT professionals involved.

Definitions

"Documents" includes, but is not limited to, writings, drawings, graphs, charts, photographs, blueprints, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained or translated if necessary.

"ESI" includes, but is not limited to, writings, drawings, graphs, charts, photographs, blueprints, sound recordings, images and other data or data compilations stored in any electronic media from which information can be obtained or translated if necessary. It includes, but is not limited to, e-mails, e-mail attachments, instant messages, word processing files, spreadsheets, pictures, application program and data files, databases, data files, metadata, system files, electronic calendar appointments, scheduling program files, TIFF files, PDF files, MPG files, JPG files, GIF files, network share files, internal websites, external websites, newsgroups, directories, security and access information, legacy data, audio recordings, voice mails, phone logs, faxes, internet histories, caches, cookies, ~~or~~ logs of activity on computer systems that may have been used to process or store electronic data, and/or Artificial Intelligence (AI) data, including but not limited to prompts, model inputs, generated outputs, and usage logs.

'Electronic media' includes, but is not limited to, hard drives (including portable hard disk drives 'HDD's'), floppy drives, disaster recovery media, and storage media (including DVD's, CD's, floppy discs, Zip discs/drives, Jazz discs/drives, USB memory drives, jump disc/drives, flash discs/drives, keychain discs/drives, thumb discs/drives, smart cards, micro-film, backup tapes, cassette tapes, cartridges, etc.), accessed, used and/or stored on/in/through the following locations: networks and servers; laptop and desktop work computers; home and personal computers; other computer systems; backup computers or servers; archives; personal digital assistants ('PDAs' – including Palm, Blackberry, cellular phone, tablet PC, etc.); pagers; firewalls; audit trails and logs, printers; copiers; scanners; digital cameras; photographic devices; and video cameras and devices. Electronic media shall also include any item containing or maintaining ESI that is obtained by the District for Board member or employee usage or that an employee uses for such purpose (even if

privately owned by the Board member or employee) from the date this policy is adopted into the future.

Initiation and Removal of a "Litigation Hold"

The Superintendent may initiate a "Litigation Hold" under this policy. Upon initiating a Litigation Hold, the District Administrator or designee shall notify the District Records Custodian to suspend disposal of records potentially covered by the hold. ~~If the District Administrator initiates a "Litigation Hold," s/he or the Board's legal counsel will notify the Board of the reason the Litigation Hold was instituted and its scope. When implementing a Litigation Hold, the Board or District Administrator ( ) may ( ) will utilize an Electronically Stored Information Team ("ESI Team").~~ The Board's legal counsel shall be involved in implementation of the "Litigation Hold Procedure".

A "Litigation Hold" shall remain in place until removed by the Board. A "Litigation Hold" may be removed when the litigation or administrative agency matter has been resolved or can no longer be initiated. Any record ~~information~~ maintained under this policy shall fall back under the "Records Retention Schedule" in Policy 8310 - Public Records once the "Litigation Hold" is removed. When a Litigation Hold is removed, the District Administrator or designee shall notify affected individuals, third parties, and records personnel that the hold has ended.

The District shall document reasonable steps taken to initiate, implement, monitor, and remove a Litigation Hold.

Custody of Third-Party and AI-Hosted Information

Records and ESI maintained in third-party hosted systems, including District-contracted AI platforms, shall be preserved in accordance with this policy **( )** and AG 8315 - Litigation Hold Procedure **[END OF OPTION]**.

Revised 4/12/21

© Neola 20 26 ~~20~~

Legal
Federal Rules of Civil Procedure 34, 37(f)

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po8330

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised STUDENT RECORDS

ADOPTED Jul 1, 2019 · REVISED May 22, 2023

8330 - **STUDENT RECORDS**

In order to provide appropriate educational services and programming, the District must collect, retain, and use information about individual students. Simultaneously, the District recognizes the need to safeguard students' privacy and restrict access to students' personally identifiable information.

Except for data identified by policy as 'directory data,' student 'personally identifiable information' includes, but is not limited to: the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number, student number, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.

Reference in this policy to 'directory data,' includes reference to 'directory information,' in the context of the Family Educational Rights and Privacy Act (FERPA).

The District is responsible for the records of all students who attend or have attended schools in this District. Only records mandated by the State or Federal government and/or necessary and relevant to the function of the School District or specifically permitted by this Board will be compiled by Board employees.

I n all cases, permitted, narrative information in student records shall be objectively-based on the personal observation or knowledge of the originator.

Any student record, or portion thereof, generated or compiled by an artificial intelligence (AI) system and/or social media/ Personal Communication Devices (PCD) communications between students and board members, staff, and/or volunteers is subject

to all provisions of this policy and all other applicable Board policies,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.

Student records shall be available only to students and their parents, eligible students, designated school officials who have a legitimate educational interest in the information, or to other individuals or organizations as permitted by law. For purposes of this policy and in accordance with FERPA, all records, files, documents, and other materials maintained by the District that are directly related to a student—regardless of format, storage location, or whether they are kept separately from the official student file—are considered education records and are accessible to parents or eligible students upon request, unless a specific legal exception applies.

Address Confidentiality Program

Students who are verified participants in the Safe at Home/Address Confidentiality Program administered by the Wisconsin Department of Justice shall be permitted to use their substitute assigned address for all District purposes. The District shall refrain from including the student's actual/confidential residential address in any student records or files (including electronic records and files) or disclosing the student's actual/confidential residential address when releasing student records. The District shall only list the address designated by the Wisconsin Department of Justice to serve as the student's address in any student records or files, including electronic records and files. Further, the District shall use the student's substitute assigned address for any and all communications and correspondence between the District and the parent(s) of the student (or adult student). The student's actual/confidential residential address shall be maintained in a separate confidential file that is not accessible to the public or any employees without a legitimate purpose. The intentional disclosure of a student's actual/confidential residential address is prohibited.

The District may enter into a memorandum of understanding with a county department under State statutes (s. 46.215, 46.22, or 46.23) or a tribal organization, as defined under Federal law, that permits disclosure of information contained in student records as provided under State law in cases in which the student's parent if the student is a minor, or the student if the student is an adult, does not grant permission for such disclosure.

The term 'parents' includes legal guardians or other persons standing in loco parentis (such as a grandparent or stepparent with whom the child lives or a person who is legally responsible for the welfare of the child). The term 'eligible student' or 'adult student' refers to a student who is eighteen (18) years of age or older.

Both parents shall have equal access to student records unless stipulated otherwise by court order or law. In the case of adult students, parents may be allowed access to the records without the student's consent, provided the student is considered a dependent under section 152 of the Internal Revenue Code, and provided that the student has not made a written request to the District that their parents not be permitted access to personally identifiable information from their records.

A school official is a person employed by the District as an administrator, supervisor, teacher/instructor (including substitutes), or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the District; a person or company with whom the District has contracted to perform a special task (such as an attorney, auditor, or medical consultant); a contractor, consultant, volunteer, or other party to whom the District has outsourced a service otherwise performed by District employees (e.g. a therapist); or a parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing tasks (including volunteers).

'Legitimate educational interest' is defined as a 'direct or delegated responsibility for helping the student achieve one (1) or more of the educational goals of the District' or if the record is necessary in order for the school official to perform an administrative, supervisory, or instructional task or to perform a service or benefit for the student or the student's family. The District directs that reasonable and appropriate methods (including but not limited to physical and/or technological access controls) are utilized to control access to student records and to make certain that school officials obtain access to only those education records in which they have a legitimate educational interest.

The District authorizes the administration to:

A. forward student records, including disciplinary records with respect to suspensions and expulsions, upon request to a private or public school or school district in which a student of this District is enrolled, seeks or intends to enroll, or is instructed to enroll, on a full-time or part-time basis, upon condition that:

    1. a reasonable attempt is made to notify the student's parent or eligible student of the transfer (unless the disclosure is initiated by the parent or eligible student; or the District's annual notification - Form 8330 F9 - includes a notice that the District will forward education records to other agencies or institutions that have requested the records and in which the student seeks or intends to enroll or is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer);

    2. the parent or eligible student, upon request, receives a copy of the record;

    3. the parent or eligible student, upon request, has an opportunity for a hearing to challenge the content of the record; and

4. no later than the next working day, the District shall transfer to another school, including a private or tribal school, or school district, all student records relating to a specific student if the transferring school district or private school has received written notice from the student (if an adult) or their parent or guardian if the student is a minor that the student intends to enroll in the other school or school district or written notice from the other school or school district that the student has enrolled or from a court that the student has been placed in a juvenile correctional facility, as defined in s. 938.02(10p), or a secured residential care center for children and youth, as defined in s. 938.02(15g);

   In this subsection, “school' and “school district' include any juvenile correctional facility, secured residential care center for children and youth, adult correctional institution, mental health institute, or center for the developmentally disabled that provides an educational program for its residents instead of, or in addition to, that which is provided by public, private, and tribal schools.

B. forward student records, including disciplinary records with respect to suspensions and expulsions, upon request to a juvenile detention facility in which the student has been placed, or a juvenile court that has taken jurisdiction of the student;

C. disclose student records that are pertinent to addressing a student's educational needs to a caseworker or other representative of the Department of Children and Families, a county department under s. 46.215, 46.22, or 46.23, or a tribal organization, as defined in 25 USC 450b(L), that is legally responsible for the care and protection of the student, if the caseworker or other representative is authorized by that department, county department, or tribal organization to access the student's case plan;

D. provide 'personally identifiable' information to appropriate parties, including parents of an eligible student, whose knowledge of the information is necessary to protect the health or safety of the student or other individuals, if there is an articulable and significant threat to the health or safety of a student or other individuals, considering the totality of the circumstances;

E. report a crime committed by a child to appropriate authorities, and with respect to reporting a crime committed by a student with a disability, to transmit copies of the student's special education and disciplinary records to the authorities for their consideration;

F. release de-identified records and information in accordance with Federal regulations;

G. disclose personally identifiable information from education records, without consent, to organizations conducting studies 'for or on behalf of' the District for purposes of developing, validating or administering predictive tests, administering student aid programs, or improving instruction;

Information disclosed under this exception must be protected so that students and parents cannot be personally identified by anyone other than a representative of the organization conducting the study, and must be destroyed when no longer needed for the study. In order to release information under this provision, the District will enter into a written agreement with the recipient organization that specifies the purpose of the study.

This written agreement must include: 1) specification of the purpose, scope, duration of the study, and the information to be disclosed; 2) a statement requiring the organization to use the personally identifiable information only to meet the purpose of the study; 3) a statement requiring the organization to prohibit personal identification of parents and students by anyone other than a representative of the organization with legitimate interests; and 4) a requirement that the organization destroy all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information must be destroyed.

While the disclosure of personally identifiable information without consent is allowed under this exception, it is recommended that whenever possible the administration either release de-identified information or remove the students' names and social security identification numbers to reduce the risk of unauthorized disclosure of personally identifiable information.

H. disclose personally identifiable information from education records without consent, to authorized representatives of the Federal government, as well as State and local educational authorities;

The disclosed records must be used to audit or evaluate a Federal or State-supported education program, or to enforce or comply with Federal requirements related to those education programs. A written agreement between the parties is required under this exception.

This written agreement must include: 1) designation of the receiving entity as an authorized representative; 2) specification of the information to be disclosed; 3) specification that the purpose of the disclosure is to carry out an audit or evaluation of a government-supported educational program or to enforce or comply with the program's legal requirements; 4) a summary of the activity that includes a description of methodology and an explanation of why personally identifiable information is necessary to accomplish the activity; 5) a statement requiring the organization to destroy all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information

must be destroyed; and 6) a statement of policies and procedures that will protect personally identifiable information from further disclosure or unauthorized use.

Under the audit exception, the District will use 'reasonable methods' to verify that the authorized representative complies with FERPA regulations. Specifically, the District will verify, to the greatest extent practicable, that the personally identifiable information is used only for the audit, evaluation, or enforcement of a government-supported educational program. The District will also ascertain the legitimacy of the audit or evaluation and will only disclose the specific records that the authorized representative needs. Further, the District will require the authorized representative to use the records only for the specified purpose and not to disclose the information any further, such as for another audit or evaluation. Finally, the District will verify that the information is destroyed when no longer needed for the audit, evaluation, or compliance activity.

I. request each person or party requesting access to a student's record to abide by Federal regulations and State laws concerning the disclosure of information.

The District will comply with a legitimate request for access to a student's records within a reasonable period of time but not more than forty-five (45) days after receiving the request or within such shorter period as may be applicable to students with disabilities. Upon the request of the viewer, a record shall be reproduced unless said record is copyrighted, or otherwise restricted, and the viewer may be charged a fee equivalent to the cost of handling and reproduction. Based upon reasonable requests, viewers of education records will receive explanation and interpretation of the records.

The District shall maintain a record of each request for access and each disclosure of personally identifiable information. Such disclosure records will indicate the student, person viewing the record, their legitimate interest in the information, information disclosed, date of disclosure, and date parental/eligible student consent was obtained (if required).

Only 'directory information' regarding a student shall be released to any person or party, other than the student or their parent, without the written consent of the parent, or, if the student is an eligible student, without the written consent of the student, except as provided by applicable law.

DIRECTORY DATA

Each year, the District Administrator shall provide a public notice to students and their parents of the District's intent to make available, upon request, certain information known as 'directory data.' The District designates as student 'directory data':

A. a student's name;

B. photograph;

C. major field of study;

D. participation in officially recognized activities and sports;

E. height and/or weight, if a member of an athletic team;

F. dates of attendance;

G. date of graduation;

H. degrees and awards received.

Parents and eligible students may refuse to allow the District to disclose any or all of such 'directory data' upon written notification to the District within fourteen (14) days after receipt of the District Administrator's annual public notice or enrollment of the student into the District if such enrollment occurs after the annual public notice. Any parent or eligible student who refuses to allow disclosure of directory data and who participates in the extra-curricular activity must complete the appropriate acknowledgement, which includes a limitation on the refusal to disclose directory data obtained during the course of the student's participation in extra-curricular activities.

In accordance with Federal and State law, the District shall release the names, addresses, District assigned e-mail addresses (if available), and telephone listings of secondary students to a recruiting officer for any branch of the United States Armed Forces or an institution of higher education who requests such information. A secondary school student or parent of the student may request in writing that the student's name, address, District assigned e-mail address (if available), and telephone listing not be released without prior consent of the parent(s)/eligible student. The recruiting officer is to sign a form indicating that 'any information received by the recruiting officer shall be used solely for the purpose of informing students about military service and shall not be released to any person other than individuals within the recruiting services of the Armed Forces.' The District Administrator is authorized to charge mailing fees for providing this information to a recruiting officer.

Whenever the consent of the parent(s)/eligible student is required for the inspection and/or release of a student's health or education records or for the release of 'directory data,' either parent may provide such consent unless agreed to otherwise in writing by both parents or specifically stated by court order. If the student is under the guardianship of an institution, the District Administrator shall appoint a person who has no conflicting interest to provide such written consent.

The District may disclose 'directory data,' on former students without student or parental consent unless the parent or eligible student previously submitted a request that such

information not be disclosed without their prior written consent.

The District shall not collect or use personal information obtained from students or their parents for the purpose of marketing or for selling that information.

INSPECTION OF INFORMATION COLLECTION INSTRUMENT

The parent of a student or an eligible student has the right to inspect upon request any instrument used in the collection of personal information before the instrument is administered or distributed to a student. Personal information for this section is defined as individually identifiable information including a student or parent's first and last name, a home or other physical address (including street name and the name of the city or town), a telephone number, or a Social Security identification number. In order to review the instrument, the parent or eligible student must submit a written request to the building principal at least fourteen (14) business days before the scheduled date of the activity. The instrument will be provided to the parent or eligible student within fourteen (14) business days of the principal receiving the request.

The District Administrator shall directly notify the parent(s) of a student and eligible students, at least annually at the beginning of the school year, of the specific or approximate dates during the school year when such activities are scheduled or expected to be scheduled.

This section does not apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for or to students or educational institutions, such as the following:

A. college or other postsecondary education recruitment, or military recruitment;

B. book clubs, magazines, and programs providing access to low-cost literary products;

C. curriculum and instructional materials used by elementary and secondary schools;

D. tests and assessments used by elementary and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments;

E. the sale by students of products or services to raise funds for school-related or education-related activities;

F. student recognition programs.

The District authorizes the use of computer data storage for the recording, filing, maintaining, and preserving of records.

No liability shall attach to any member, officer, or employee of this Board as a consequence of permitting access or furnishing student records in accordance with this policy and regulations.

Any entity receiving personally identifiable information pursuant to a study, audit, evaluation, or enforcement/compliance activity must comply with all FERPA regulations. Further, such an entity must enter into a written contract with the District delineating its responsibilities in safeguarding the disclosed information. Specifically, the entity must demonstrate the existence of a sound data security plan or data stewardship program, and must also provide assurances that the personally identifiable information will not be redisclosed without prior authorization from the District. Further, the entity conducting the study, audit, evaluation, or enforcement/compliance activity is required to destroy the disclosed information once it is no longer needed or when the timeframe for the activity has ended, as specified in its written agreement with the District.

Revised 11/25/19

Revised 4/12/21

Revised 4/23/22

Revised 12/12/22

© Neola 20 26 ~~22~~

Legal
46.215, Wis. Stats.
46.22, Wis. Stats.
46.23, Wis. Stats.
115.298, Wis. Stats.
118.125, Wis. Stats.
118.125(2)(q), Wis. Stats.
20 U.S.C. Section 1232f (FERPA)
20 U.S.C. Section 1232g (FERPA)
20 U.S.C. Section 1232h (FERPA)
20 U.S.C. Section 1232i (FERPA)
20 U.S.C. 1400 et seq., Individuals with Disabilities Education Improvement Act
20 U.S.C. 7165(b)
20 U.S.C. 7908
25 U.S.C. 450b(L)
26 U.S.C. 152
34 C.F.R. Part 99

ARTIFICIAL INTELLIGENCE (AI) SPECIAL UPDATE

po8330.01

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised UNAUTHORIZED ACQUISITION OF STUDENT PERSONAL INFORMATION

ADOPTED Jul 1, 2019

8330.01 - **UNAUTHORIZED ACQUISITION OF STUDENT PERSONAL INFORMATION**

The District is responsible for maintaining records of all students attending schools in this District.

If the District becomes aware of the unauthorized acquisition of "Personal Information", including acquisition facilitated by an Artificial Intelligence (AI) system or its associated vendor platform, the District shall make reasonable efforts to notify each affected student, and if a minor, the parents, that their personal information has been accessed.

"Personal Information" includes the individual's social security number, driver's license number, State identification number, the number of financial accounts or access codes, the individual's deoxyribonucleic acid (DNA) profile, or the individual's unique biometric data including fingerprint, voice print, retina or iris image, or any other unique physical representation.

The notice shall be issued within a reasonable time, not to exceed forty-five (45) days after the District learns of the acquisition of the personal information. The notice shall indicate that the District knows of the unauthorized acquisition of personal information pertaining to the student. The notice shall be by mail or by a method the District has previously employed to communicate with the students.

If, as the result of a single incident, the District is required to notify 1,000 or more students, the District shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices sent to the students. Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.

Upon written request from the student who has received a notice, the District shall identify the personal information that was acquired.

A law enforcement agency may, in order to protect an investigation or homeland security, ask the District not to provide a notice for any period of time and the District's notification process shall begin at the end of that time period.

© Neola 20 26 ~~09~~

Legal

~~134.98 Wis. Stats.~~
134.98(2)(cm)(1)(2), Wis. Stat.