

Book	Policy Manual
Section	FOR BOARD APPROVAL - Special Update - Artificial Intelligence June 2026
Title	Updated Copy of ARTIFICIAL INTELLIGENCE
Code	po7540.09
Status	
Adopted	March 18, 2025

7540.09 - **ARTIFICIAL INTELLIGENCE ("AI")**

The School Board recognizes the positive impact that artificial intelligence ("AI") technology may have on the School Corporation's educational program and operations. The Superintendent is authorized to support the use of AI technology when its use is consistent with the Corporation's mission, goals, and operational integrity.

Any use of AI technology in the Corporation'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: Board Policy 2266—Nondiscrimination on the Basis of Sex in Education Programs and Activities; Board Policy 5136—Personal Communication Devices; Board Policy 5500—Student Conduct; Board Policy 7540.03—Student Technology Acceptable Use and Safety; Board Policy 7540.04—Staff Technology Acceptable Use and Safety; Board Policy 8330—Student Records; Board Policy 8350—Confidentiality; and Board Policy 8351—Security Breach of Confidential Databases.

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 Administration will refer any illegal acts to law enforcement.

The School Board 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 Corporation's mission, goals, and operational integrity. The Superintendent and Technology Director are 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 output, from text and images to music and code, that mimic the system or characteristics of the data on which it was trained.

At its core, generative AI predicts the flow of language. Trained on massive amounts of text taken from publicly available internet sources to recognize relationships that most commonly exists 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 Corporation, its staff, or its operations. This information is considered the Corporation'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 Corporation contract, they present a high risk of data exposure.

- A. **Shared Data:** Data input into these tools is frequently used to train global models, making the information publicly available or accessible to the provider.
- B. **Lack of Filtering:** These models may require the Corporation to manually implement its own "wrapper" or filtering layers to manage safety.

- C. **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 Indiana Access to Public Records Act), the use of Public-Domain AI is prohibited for any task involving student records, personally identifiable information (PII), or confidential Corporation operations.

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:

- A. **Guarantees Data Privacy & Security:** Ensures all Corporation data remains isolated within a private "tenant" or environment.
- B. **Prohibits Model Training:** Strictly ensures that Corporation data, including student and staff information, is not used to train the provider's global models.
- C. **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 Corporation 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 Corporation-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 Corporation infrastructure. The Corporation 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 explicit written approval from the IT Department 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, professional work, or used to influence and/or make decisions. () 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**

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

C. Content Responsibility

Corporation 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 Corporation'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 2240—Controversial Issues; Policy 2260—Nondiscrimination and Access to Equal Educational Opportunity; Policy 2260.01—Section 504/ADA Prohibition Against Discrimination Based on Disability; Policy 2266—Nondiscrimination on the Basis of Sex in Education Programs and Activities; Policy 5136—Personal Communication Devices; Policy 5500—Student Conduct; Policy 5517—Anti Harassment; Policy 5517.01—Bullying; Policy 7540.03—Student Technology Acceptable Use and Safety; Policy 7540.04—Staff Technology Acceptable Use and Safety; Policy 8310—Public Records; Policy 8330—Student Records; Policy 8350—Confidentiality; and Policy 8351—Security Breach of Confidential Databases. **[DRAFTING NOTE: Confirm and Select as Needed]**

AI Tool Approval

The Corporation will approve the use of Public-Domain AI, Enterprise-Grade, Locally Hosted AI tool(s) once each tool has been reviewed and verified for compliance with Federal law, State statute, and Board policies.

AI Tool Evaluation

Before adopting any AI tool or system, the Corporation will conduct a comprehensive risk assessment - evaluating data sources (including use of student PII), 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, Indiana statutes, and Corporation 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 Corporation approves the use of AI tools as delineated in the policy, that have been carefully reviewed, evaluated, and approved by the Technology Director for student and staff use.

Transparency

The Corporation 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 the Technology Director, and conducting regular audits to evaluate accuracy, fairness, and impact on equity and student rights. The Corporation 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 Corporation must undergo a formal risk assessment by the IT/Legal Department to review their terms of service and data handling practices to ensure compliance with all Federal and State privacy laws. The Corporation 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.

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 Corporation policies, including but not limited to FERPA (34 CFR Part 99), the DPA technically and legally must enforce the following:

- A. **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 Corporation regarding the use and maintenance of all education records.
- B. **Data Ownership & Custody:** The Corporation 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 Corporation-provided PII.
- C. **Prohibition on Model Training:** The Vendor must provide a "Zero-Retention" or "Private Tenant" guarantee, ensuring that Corporation 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.
- D. **Security & Breach Notification:** The Vendor must employ industry-standard encryption (AES-256 or higher) and provide immediate notification within seventy-two (72) hours of any suspected unauthorized acquisition of student PII, in alignment with Policy 8351 - Security Breach of Confidential Databases.
- E. **Right to Audit & Deletion:** The Corporation 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 Corporation data within thirty (30) days.

Employee Use of AI

- A. **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 Corporation-approved AI applications/tools.
- B. **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.
- C. **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. If an employee intends to enter PII or sensitive or proprietary data into an AI tool, they first must ensure the tool is on the Corporation's Approved AI Tool Inventory. If it is not, they must seek written approval from their Principal, who will consult with the IT Department regarding legal and privacy safeguards.
- D. **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 also must disclose the use of AI software in course curricula.
- E. **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.
- F. **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, and State or Federal laws. The Corporation is fully responsible for the accuracy, security, access, and disclosure of all AI-generated content within a record, as if created solely by a Corporation employee. (See Policy 8310 - Public Records and Policy 8330 - Student Records.)
- G. **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

- A. **Instruction:** Students shall receive age-appropriate instruction about responsible AI use, digital citizenship, privacy, and the risks/limitations of AI prior to using AI.
- B. **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 disclosed properly 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).
- C. **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 Conduct and other applicable Board policies.
- D. **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 Conduct. **[DRAFTING NOTE: Confirm the Board has adopted this policy if referenced.]** AI-detection results shall not serve as the sole basis for a finding of academic dishonesty without additional corroborating evidence or student inquiry.
- E. **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 individualized education program (IEP).

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 the 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 Corporation.

Non-Academic Use of AI

Students and staff are prohibited from using AI to generate false or knowingly misleading representations of other students, staff, administrators, 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 Administrator 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 Corporation should contact the Technology Director.

© Neola 2024

Cross References	po2266 - NONDISCRIMINATION ON THE BASIS OF SEX IN EDUCATION PROGRAMS OR ACTIVITIES
	po5136 - PERSONAL COMMUNICATION DEVICES
	po5500 - STUDENT CONDUCT
	po7540.03 - STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
	po7540.04 - STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY
	po8330 - STUDENT RECORDS
	po8350 - CONFIDENTIALITY
	po8351 - SECURITY BREACH OF CONFIDENTIAL DATABASES