ILLINOIS
STATE BOARD OF
EDUCATION

Policy on the Acceptable and Responsible Use of Artificial Intelligence

1. Background & Introduction

Recent federal guidance prioritizes minimal government interference, and a strong free-market approach to Artificial Intelligence ("AI") regulation (Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence"). Further, the federal "Blueprint for an AI Bill of Rights" states that AI systems should be designed, developed and deployed according to principles that bolster democratic values, protect civil rights, preserve civil liberties, and ensure privacy. Considering this shift in regulatory philosophy and with no stable national framework in place, state legislatures like Illinois' are increasingly establishing their own policies and rules around AI usage, privacy, ethics, and accountability. For example, Illinois passed the Artificial Intelligence Video Interview Act (820 ILCS 42/5) and the Wellness and Oversight for Psychological Resources Act (Public Act 104-0054). Illinois has proposed numerous additional AI bills, which would regulate AI as it applies to insurance, consumer protection, consumer financial services, and other business sectors.

This Policy (this "Policy") outlines the acceptable and responsible use of artificial intelligence systems and technologies ("AI"), as defined below, within the Illinois State Board of Education ("ISBE" or the "Agency"). AI offers significant potential benefits to Illinois residents by both improving public services and enhancing state operational efficiency, while safeguarding citizens' rights and privacy and adhering to ethical principles, such as fairness, transparency, accountability, and data protection.

This Policy is intended to govern ISBE's development, adoption, use, deployment, and oversight of AI systems while mitigating potential risks. Entities associated with the development, deployment, and use of AI systems (as defined below) may be broadly divided into two categories: (1) those who create AI systems, including related algorithms, models, and data ("AI Creators"); and (2) those who use or consume those AI systems ("AI Consumers"). While the compliance aims and obligations of both groups will have significant overlap, the requirements to achieve those aims and obligations may differ. AI development, use, deployment, and governance must be aligned with state law and applicable privacy, ethical, and technology standards. The following is a structured approach adapted to meet the state's legal and ethical requirements.

2. Scope & Authority

This Policy applies to all officials, staff, employees, contractors, and agents of ISBE in their potential roles as AI Consumers, AI Creators, or both — by addressing any AI systems that may be developed, adopted, used, or deployed by ISBE. This Policy has been reviewed and approved by ISBE Leadership and Legal Department and will take effect immediately upon execution. For AI systems that on the effective date of the Policy are already deployed, in active development, or in use, Departments shall have ninety calendar days to either bring such systems into compliance or develop a plan with a definite timeline to bring such systems into compliance. Many of the requirements and concepts below directly relate to the Agency's own mission and existing compliance obligations. Compliance with this Policy depends on each department's specific needs, and existing compliance obligations related to protected or sensitive information collected, held, or used, including personally identifiable information ("PII") contained in education records protected by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) ("FERPA") and the Illinois School Student Records Act (105 ILCS 10/1, *et seq*.) ("ISSRA").

3. Definitions

- **Artificial Intelligence (AI)**: Refers to the use of computer programs that can perform tasks traditionally requiring human intelligence, such as problem solving, decision making, predictions, recommendations, ongoing learning, etc. The use of AI, as covered by this Policy, includes machine learning, natural language processing, deep learning, neural networks, large language models, algorithmic decision support, pattern recognition, anomaly detection, computer vision, generative AI, and similar functionality.
- **AI System**: Any software, system (physical or virtual), or application that uses AI, in whole or in part, to perform tasks (examples include virtual meeting assistants, digital voice assistants, customer service chatbots, facial recognition software, and writing assistant services, among others).
- **Generative AI**: A type of AI model that emulates the structure and characteristics of input data to generate derived synthetic content, which may include images, videos, audio, text, other digital content, or various combinations of the above.
- **AI Assistant, Extension, or Transcription Tool**: An AI tool that uses AI technology to enhance meetings with features like summarization and integrations with platforms like Microsoft Teams, Zoom AI Companion, and Otter.ai. Such tools also provide automated notetaking, scheduling, speaker identification and follow-up tasks.
- **Machine Learning (ML)**: Algorithms that learn patterns from data without explicit programming.
- **Natural Language Processing (NLP):** AI methods for understanding, interpreting, and generating human language.
- **Neural Network**: Computational model inspired by biological neurons.
- **Training Data**: Refers to data used to build, tune, test, and validate an AI system. Some models will require the use of operational data to periodically or continuously train and/or re-train.
- **Operational Data**: Refers to data input, used, or generated (either directly or indirectly) when an AI system is deployed and generates outputs in a live environment. Such data would include user prompts, feedback or data related to user interaction and system telemetry, and drift monitoring. Operational data may be used for additional or as performance indicators related to retraining needs.

- **Protected Dat**a: Protected data means any information or data owned and maintained by ISBE that is protected under law or regulation or that is sensitive, confidential, or otherwise prohibited from disclosure, including personally identifiable information ("PII") contained in education records protected by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) ("FERPA"), the Illinois School Student Records Act (105 ILCS 10/1, et seq.) ("ISSRA"), the Children's Online Privacy & Protection Act (15 U.S.C. § 6501-6506) ("COPPA"), the Children's Internet Protection Act (47 U.S.C. § 254) ("CIPA"), the Children's Privacy Protection and Parental Empowerment Act (325 ILCS 17/1), the Individuals with Disabilities Education Act (20 U.S.C. § 1400) ("IDEA"), 105 ILCS 5/14-1.01 *et seq*., the Illinois Freedom of Information Act (5 ILCS 140)("FOIA"), the Performance Evaluation Reform Act (105 ILCS 5/24A-1 *et seq.*) ("PERA)", the Privacy Act of 1974, 5 U.S.C. § 552a, the Social Security Act (42 U.S.C. §§ 1320d-2 through 1320d-7), the Student Online Personal Protection Act (105 ILCS 85/1 *et seq*.)("SOPPA"), Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.*, ("BIPA"), Identity Protection Act (5 ILCS 179/1 *et. Seq*.), the Personal Information Protection Act (815 ILCS 530/*et seq*.) ("PIPA)", the Data Processing Confidentiality Act (30 ILCS 585/0.01), and other applicable state and federal laws.
- **Bias:** Refers to systematic and unfair outcomes resulting from AI systems, including disparate impact on protected groups. (See NIST March 2022 Special Publication 1270 publication, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence.)

4. Ethical Requirements

AI systems shall not:

a. **Discriminate:** AI systems shall not be used, developed, or deployed in ways that could potentially discriminate or reinforce discriminatory outcomes against individuals or groups of people based on race, gender, religion, ethnicity, disability, economic status, or any other protected characteristic.

b. **Infringe Privacy:** AI systems shall not violate relevant data privacy laws and regulations but instead must ensure the secure and responsible handling of PII and avoid copyright infringement.

c. **Mislead or Manipulate:** AI systems shall not be used to spread false or misleading information, deceive users, or manipulate public opinion.

d. **Make Decisions Without Oversight:** AI systems shall not make decisions autonomously without oversight. AI systems must have a "human in the loop" to ensure that all decisions are reviewed, finalized, and made by humans.

e. **Violate Human Rights:** AI systems shall not be used to undermine or cause harm to fundamental human rights. Potential human rights risks could include unlawful and/or inaccurate surveillance and tracking, including inappropriate algorithmic management and AI-enabled workplace monitoring.

f. **Access Protected, Sensitive, or Confidential Information:** AI systems shall not, without written authorization signed by the Chief Information Officer, directly or indirectly have access to any information or data that is protected under law or regulation (including but not limited to, PIPA, FERPA, PERA, etc.), or that is sensitive, confidential or otherwise protected from disclosure including protected data safeguarded under this Policy. In the event the Chief Information Officer authorizes the AI system to access protected data, ISBE must ensure the following throughout the duration of such access and on an ongoing basis afterwards:

   i. AI system is and remains fully contained in, and its access to and use of the Protected Data occurs entirely within a separate, private environment.

   ii. Protected data to which the AI System has direct or indirect access does not become part of a public model or dataset, in any form; and

   iii. AI system shall not reproduce or generate any output that embeds or otherwise includes the protected data, or make any decisions based on such protected data, unless the Chief Information Officer grants explicit, written authorization to do so. If an AI system is allowed to include protected data in its output or decision making, the system may do so only exactly as allowed.

5. Transparency and Accountability

b. **Clear Communication:** When users interact with an AI system, the Agency shall disclose to those users that they are interacting with an AI system.

c. **Disclosures:** ISBE must disclose the use of AI in any products and services upon which the Agency relies. This disclosure must contain a full and clear description of how AI is used in the applicable products and services and must be communicated in writing to the users of those products and services. **Users must have an option to opt out of an AI system in favor of a human alternative.**

d. **Explanation of Decision Making:** When an AI system is used to support decision making, the Agency shall disclose and make available the role of the AI system in supporting decision making.

e. **Human Oversight**: AI systems shall have appropriate and ongoing human oversight to review and intervene in cases of potential bias, errors, or potential adverse impacts. To achieve this, departments shall define and assign clear oversight roles and responsibilities to applicable personnel for the entirety of an AI system's lifecycle to ensure its development, deployment, and/or use align with Illinois's legal and regulatory frameworks. Such oversight roles must be documented, assigned, and auditable. The mechanisms for ensuring human oversight will be defined on a per project basis, and the elements and procedures for human oversight will be enumerated in the process of applying for use or development of an AI system.

f. **Data Management:** ISBE shall only use high-quality, trusted, and vetted data sources. ISBE shall not allow the use of the state of Illinois data in any way for AI-related purposes (including but not limited to model building and inference reference), without the express written consent of ISBE's Chief Information Officer in compliance with Illinois law.

g. **Accountability**: To secure permission to use any AI system, prior to such use, the appropriate Department Director or Executive Director will assess the AI system's adherence to this Policy and create a written report documenting the findings and conclusions of the assessment. The precise workflow depends upon the source and type of request as follows:

   i. For third-party software requests, the request must be submitted via the ServiceNow Portal and vetted by the Technology Support and Infrastructure (TSI) Director for compatibility, security, audit compliance, and alignment with this Policy. If deemed suitable, the TSI Director will submit the findings to the Chief Information Officer for final review and approval.

   ii. In the case of AI development projects, the process begins with a CAF submission and TSI Director review. If in the process of that review, AI functionality is identified, Procurement will be notified that no award may proceed until the proposal has been evaluated for compliance with cybersecurity, SOC standards, AI policy, and infrastructure compatibility. Final approval will rest with the Chief Information Officer following Information Technology's review of the selected proposal.

   iii. If the TSI Director were to initiate an AI system request, the Director shall provide compliance assurances and consult with the Chief Information Officer for approval prior to procurement and implementation.

   iv. In all cases, a written summary documenting the assessment findings and conclusions shall be prepared and submitted to the Chief Information Officer. No AI system may be deployed or procured without the Chief Information Officer's approval.

6. Use of AI Extensions or Transcription Tools

The internal use of AI assistants, extensions, or tools during meetings is generally permitted; however, only approved AI tools shall be used. AI Assistants shall be reviewed for cybersecurity and privacy by the Chief Information Officer and approved for Agency use pursuant to a written agreement between ISBE and the AI vendor. Although ISBE may restrict the internal use of AI extensions, ISBE cannot prevent external or third-party participants from using them on personal or district-issued devices. These tools are generally installed on client applications outside of the

Agency's control, and the Agency lacks the resources to vet every AI assistant in use. Some tools may claim to process data locally, but many transmit and store information with third-party vendors, raising privacy and compliance concerns.

a. **Notification and Consent**; AI extensions do not always notify all meeting attendees when active. Therefore, it is essential to provide advance notice to all participants that AI tools will be used during the meeting. Illinois law requires the consent of all participants in meetings, whether a meeting is with external participants or solely an internal meeting. Under the Illinois Eavesdropping Statute (720 ILCS 5/14-2), recording a private conversation without the consent of all parties is illegal — even if you are one of the people involved in the conversation. In People v. Ceja, 204 Ill. 2d 332 (Ill. 2003), the Supreme Court of Illinois held that under the Illinois Eavesdropping Statute, 720 ILCS 5/14, consent may be expressed or implied. If a meeting participant objects to the use of an AI assistant or extension, the meeting may not be recorded, and the host must disable AI features if a meeting participant requests that features be turned off while presenting or asking questions. Note that government/board meetings under the Open Meetings Act (5 ILCS 120/2.05) ("OMA") are open to recording by the public; therefore, all-around consent is not required for such public meetings. Internal, routine agency meetings or closed session board meetings that are not open meetings under the OMA would be covered by the Illinois Eavesdropping Statute, 720 ILCS 5/14. As such, all-party consent (either explicit or implicit) is required.

See below disclaimer which may be added to a meeting invitation or included at the top of the calendar invitation, if any. (*The only exception would be to accommodate a disability, which in that case, the expectation is the external party must notify the staff in advance of the meeting so that proper measures can be taken, such as obfuscation or redaction of confidential information.)*

> *"To maintain the integrity and confidentiality of this meeting, the use of AI assistants, extensions, or transcription tools is not permitted. If you are using an AI tool, please disable it before joining. Attendees who do not comply may be removed from the meeting.*
>
> *In accordance with the Americans with Disabilities Act (2 U.S.C. § 12101 et seq.,) (ADA)and Section 504 of the Rehabilitation Act of 1973 (29 USC 793, et seq., 49 CFR 2), accommodations are available upon request. If you require accessibility support to fully participate in this meeting, please contact [insert contact name/email] at least 48 hours in advance.*
>
> *Thank you for your cooperation and commitment to an inclusive and secure meeting environment."*

If an external user is using an AI assistant, this feature should be disabled. If they are unable or unwilling to do so, they must be removed from the meeting to ensure compliance with ISBE's data protection and data security standards and meeting integrity.

Many AI assistants will show up in a meeting as a second attendee. A duplicate name may appear in the participants list, e.g., Joe Harrison-AI. If these names should appear, remove them from the meeting.

Individuals may not "send" an AI assistant to "attend" a meeting on their behalf when the individual is not also present. No one may require individuals to "send" an AI assistant to "attend" on the absent individual's behalf.

b. **Sensitive or Confidential Information**. Use of an AI assistant shall be prohibited in meetings involving privileged, confidential, or sensitive information (e.g., personally identifiable information ["PII"], investigations, employee performance data, funding proposals, or confidential materials, intellectual property not publicly released, performance reviews, legal strategy discussions, and similar settings). However, any use of AI involving Human Resources records during employee disciplinary meetings or meeting discussing alleged misconduct by ISBE employees is subject to the requirements of HB 3773, and a written agreement between ISBE and the AI vendor. AI tools may be used during internal meetings involving ISBE intellectual property (e.g., Software Solutions developers may use an AI assistant during a meeting discussing proprietary design documents, only in cases where the AI assistant has been approved for Agency use pursuant to a written agreement between ISBE and the AI vendor, which will serve to safeguard ISBE's proprietary information.)

    i. Attorney-Client Privilege. Avoid potentially losing the protection of the attorney-client privilege; AI note-taking tools should not be used to document meetings with the legal counsel.

    ii. Private information. Using AI note-taking tools for meetings involving students may violate the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) ("FERPA") and the Illinois School Student Records Act (105 ILCS 10/1, et seq.) ("ISSRA"), which prohibit school officials from disclosing a student's education records or personally identifiable information from those records without written consent from a parent or eligible student (an adult student or emancipated minor). The definition of "personally identifiable information" includes most information in an education record that is linked or linkable to a specific student (34 CFR §99.3). Education records are those that contain information directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution.

School officials often discuss sensitive student matters during meetings, and AI note taking may compromise student privacy. For example, if school officials use an AI note-taking tool during an Individualized Education Program team meeting, that student's information will likely be stored on the tool's server and could be disclosed to third parties in violation of FERPA and the Individuals with Disabilities Education Act (20 U.S.C. § 1400) ("IDEA").

7. Deciding on Human Involvement

a. **Workflow and Processes**: At every stage of the AI system adoption process, from proposal and case creation to design and implementation, to usage and review, ISBE shall establish documented protocols for human oversight and/or intervention in automated, or partially automated, AI processes. To ensure efficient human oversight and intervention:

   i. In the foundational documents of AI system develop, such as the project plan, statement of work, and/or design documents, the scope of the project will be outlined in detail. These documents will explicitly discuss what processes will be automated versus those reviewed by human staff and justify the choices made.

   ii. Human ISBE staff will regularly review AI system output before final action is taken. The cadence and method of human review must also be detailed in foundational, case-making documents.

   iii. Structure the workflow in such a way that prefers human oversight over intervention wherever possible. To the extent possible, human ISBE staff shall supervise AI system work in real time, rather than after the fact.

8. Maintaining, Monitoring, Documenting, and Reviewing Agency Data Use and Access for AI Systems

a. **Monitoring and Maintenance:** ISBE shall implement continuous monitoring and maintenance protocols for use of and access to Agency data in AI systems, ensuring they comply with Illinois law and any laws and regulations applicable to an Agency's data over time. This monitoring may be automated and inherent in an AI system, or it may be done as part of human oversight over any AI system:

   i. Automatic oversight may include, but is not limited to, access logs, system health dashboards ensuring the system is operating as intended, system updates, system backups, which may be automated or initiated by the Technology Support and Infrastructure Department.

   ii. Manual, human-led maintenance and documentation may include, but is not limited to, review of Illinois or federal laws that may dictate changes to an AI system, user access reviews by the program area, change logs detailing changes made to the system, and/or spot checking for accuracy in the AI system output.

b. **Change Management**: ISBE shall extensively document AI systems' design, development, deployment, and any modifications with respect to the use of and access to Agency data, promoting transparency and accountability in line with Illinois law.

9. Reviewing Communication and Feedback Mechanisms

a. **Communication:** ISBE shall maintain transparent communication channels with stakeholders regarding the use of AI, ensuring compliance with applicable Illinois law. Communication will be in writing to ensure clarity and to create a documented record of communication.

b. **Feedback**: ISBE shall develop feedback mechanisms for stakeholders to report AI-related concerns or issues, especially those affecting legal rights within Illinois.

10. Organizational Awareness

a. **Internal Communication**: ISBE shall promote organization-wide awareness of AI's legal, ethical, and operational aspects, emphasizing the importance of escalating issues to experts familiar with Illinois law, including, but not limited to, ISBE's Legal Department.

11. Data Usage and Privacy

a. **Data Quality:** ISBE shall ensure that data collected for use by AI systems must be relevant, accurate, and necessary for the intended purpose.

b. **Data Minimization**. Only the data necessary for the specific purpose shall be collected and access to that data shall be limited.

c. **User Consent**. If required by law, express consent from individuals shall be obtained before using their data in AI systems.

d. **Data Use**: When using AI systems that rely on analysis of large amounts of data to provide insights, the Agency is responsible for the quality and governance of the **training data** it selects to be used to support the AI system.

12. Fairness and Bias Mitigation

a. **Corrective and Preventative Actions:** ISBE shall conduct and document reviews at least annually to ensure that their AI systems are free from potential biases, taking necessary corrective and preventative actions upon bias detection.

b. **Documentation**: ISBE must document all processes and changes made to any algorithms governing an AI system to ensure diverse and representative **training data**.

13. AI System Security Reporting

AI poses risks due to potential misuse, flawed design, inadequate governance, and other factors. Without proper governance and security controls, some uses of AI can lead to unintended results, including data privacy or cybersecurity vulnerabilities, ethical or civil rights violations, and disparate impacts. Moreover, the technical aspects of many AI application mechanics are not fully understood, and this poses a unique challenge to state agencies, such as ISBE, that serve the public. To ensure robust security measures are in place for AI systems and to establish a reporting mechanism for security incidents, see below procedures.

Awareness: All employees, contractors, and relevant stakeholders shall be made aware of the reporting process and its importance in ensuring the security of AI systems. This shall be achieved through regular training, email reminders, and onboarding sessions.

a. **Reporting Method:** Any concerns or potential violations related to AI systems, including timelines and responsible parties, may be sent directly to the ISBE Security team: infosec@isbe.net.

b. **Acknowledgment:** Upon receiving a report, the ISBE Security team will acknowledge its receipt, ideally within 24 hours. This acknowledgment reassures the submitter the concern is being addressed.

c. **Evaluation:** The ISBE Security team will evaluate the report to determine its severity, potential impact, and necessary actions.

d. **Feedback Loop:** Once an evaluation is completed and necessary actions are taken, the ISBE Security team will provide feedback to the submitter. This feedback will cover the outcome of the evaluation and any measures taken in response.

e. **Remediation:** If a genuine security concern or violation is identified, the ISBE Security team will:

   i. Coordinate with relevant teams to fix the issue.

   ii. Revise this Policy and other current AI security guidelines, if needed.

   iii. Conduct an incident review to identify lessons learned and to avoid similar issues in the future.

f. **Documentation:** Maintain a record of all reports, evaluations, actions taken, and outcomes. This not only ensures compliance and transparency, but also helps in refining the AI security posture over time.

g. **Continuous Improvement:** At least annually, review and refine the reporting process based on feedback and emerging AI security challenges. Ensure stakeholders are informed of any changes to the reporting process.

h. **Confidentiality**: All reports will be treated with utmost confidentiality. The identity of the reporter shall be protected unless they give explicit consent for disclosure.

14. Compliance and Reporting

Non-compliance with this Policy may result in exposure to risk and liability to the state. Concerns or potential violations related to AI systems should be reported as outlined above. Reports and notices required by this Policy should be submitted to the ISBE Security team at the designated email address.

15. Contact Information and Additional Information

For questions or clarifications regarding this document, please contact ISBE Security at InfoSec@isbe.net.

ISBE Acceptable Use Policy

LAST REVIEWED OR UPDATED:

Date	Manager	Updates
11/06/25	Edobor Efam, Information Technology	Released