

Boston Public Schools Artificial Intelligence (AI) Policy

I. Vision, Core Values, and Guidelines

Vision

Boston Public Schools (BPS) is committed to the responsible, ethical, and effective use of Artificial Intelligence (AI) to support teaching, learning, and district operations. AI is a tool to support and enhance, not replace, human judgment, professional expertise, and critical thinking. This policy establishes district-wide expectations for the safe and appropriate use of AI by staff and students. It is grounded in our commitments to student learning, data privacy, and transparency.

AI technologies are rapidly evolving and may produce inaccurate, biased, or incomplete outputs. As such, AI-generated content must be reviewed critically and used with professional and academic judgment. AI must not be used as the sole basis for decisions that significantly impact students or staff, including grading, placement, discipline, or evaluation.

Core Values

BPS recognizes both the opportunities and risks of AI and is committed to implementing this policy grounded in the following core values:

- **Human-Centric Approach:** AI will support and enhance - *not replace* - human connection, collaboration, and capabilities. Educators, staff, and students remain responsible for all decisions and outputs.
- **Safety, Privacy, & Security:** The protection of student and staff data is paramount. AI systems and tools must meet district standards for [data privacy, security, and compliance](#).
- **Equity & Inclusion:** AI must be designed and implemented thoughtfully to promote equitable access to educational opportunities for all students, regardless of background or learning needs. This also includes cultivating the awareness that AI can reinforce harmful stereotypes, misrepresent cultures, infer bias, and contain inaccuracies.
- **Responsible Use:** AI tools should be used in a manner that is socially responsible, safe, and legal. This includes prioritizing privacy and security of student and staff data, being mindful of potential biases or misinformation, and avoiding overreliance.
- **Purposeful Use:** AI should be used to support meaningful goals, improve experiences for students and staff, and reflect our values. We recognize its risks, including bias, overreliance, and environmental impact, and commit to using AI only when it adds clear value to teaching, learning, or district operations.
- **Transparency & Explainability:** Students and staff must disclose when AI is used and explain, to the extent possible, how AI contributed to a decision or output.
- **Continuous Learning:** BPS will continuously evaluate AI tools and practices and update our guidance and policy as technology evolves.

AI Guidelines

For day-to-day operational guidance, classroom application, and practical decision-making, educators, students, families, and staff should reference the [BPS AI Guidelines](#).

II. Governance, Data Privacy, and Security

Implementation Responsibility

The District will maintain a centralized list of all approved [AI tools](#), provide required training, and establish guidelines for implementation. School leaders are responsible for ensuring staff understand and consistently apply this policy. All staff and students are responsible for adhering to these expectations.

Procurement and Vendor Oversight

- **Mandatory Vetting:** All AI tools must undergo a Privacy Impact Assessment (PIA) for compliance with FERPA (Family Educational Rights and Privacy Act), COPPA (Children's Online Privacy Protection Act), and District security standards. *Visit our [website](#) to learn about the approval process.*
- **Data Ownership:** District data remains District property and cannot be used by vendors to train public AI models. To ensure compliance with this principle, contracts must include language noting this requirement.
- **Vendor Disclosure:** Vendors are required to disclose AI capabilities within their products, including updates that add AI functionality to existing portals and/or tools.
- **Technical Control:** The District must retain the ability to enable, disable, or restrict specific AI functionalities within any adopted software.

Use of AI with Student and Staff Data

Students and staff may only use AI tools that have been reviewed and approved by the District and included on the District's published list of approved AI tools.

- **Prohibited Use:** Under no circumstances may students or staff enter personally identifiable information (PII), including student names, IDs, IEPs, 504 plans, health records, or any confidential information, into unapproved AI tools (e.g. open AI platforms or personal accounts).
- **Responsibility:** All users are responsible for protecting student data. When in doubt, users must not input data into an AI tool and should seek guidance from the Office of Technology.
- **Use of Non-Approved Tools:** The use of personal, non-approved AI tools for school-related work is prohibited when it involves district data or student information.

For more information about student data privacy, read [BPS Superintendent Circular ODA-03](#).

Bias and Unintended Outcomes

AI systems may produce outputs that reflect bias, inaccuracies, or unintended harmful impacts due to limitations in data or design. BPS requires that:

- AI outputs used for instruction, grading, communication, or decision-making are reviewed for bias, accuracy, and appropriateness.
- AI must not be used in ways that disadvantage individuals or groups based on protected class.

- Students and staff are trained on AI literacy and taught to evaluate AI-generated content and identify potential bias and misinformation.

Security

- **Secure Logins:** Access to AI systems containing sensitive data will be governed by single-sign on, role-based access controls and multi-factor authentication (MFA).
- **Data Breaches:** The District will follow its cybersecurity protocols for any AI-related breaches.

III. AI in Teaching, Learning, and Professional Practice

AI Literacy and Training

Responsible use of AI requires foundational knowledge and ongoing learning. BPS will require students and staff to be trained in AI literacy, which is the ability to understand, evaluate, and use AI technologies in a responsible, safe, and effective manner, regardless of whether you use AI tools or not. AI literacy is a necessary skill for all staff and students because we are all exposed to AI-generated content and impacted by AI-driven decisions.

- **Staff Training:** All new staff will complete required training on AI use, including data privacy, bias, instructional use, and ethical considerations. Ongoing professional learning will be provided throughout the year as technology, tools, and expectations evolve.
- **Student Learning:** Students will receive age-appropriate instruction on AI literacy, including how AI works, its limitations, and how to use it both responsibly and critically. Before using AI tools for an assignment, students should first receive foundational AI literacy instruction from a teacher at their school.
- **Family Support:** BPS will provide resources to support families in understanding AI use, risks, and expectations.

Use of AI Tools for Instruction

- AI may be used to support differentiation, feedback, and instructional planning with district-approved curriculum. All AI use must maintain academic rigor, uphold learning standards, and reinforce the integrity of the human-led teaching and learning process.
- Educators and staff must apply their professional expertise to review AI-generated outputs before use, ensuring accuracy, developmental appropriateness, inclusivity, and ethical application.

Use of AI Tools for Grading & Assessment

AI must not be used as the sole basis for grading, discipline, or academic evaluation. Teachers using AI tools for grading and assessment must exercise human judgment, transparency, and be able to explain how and why they used an AI tool. AI tools should not be used to make final decisions about student grades, placement, or evaluation.

- **Use of AI Detection Tools:** AI detection tools must not be used as the sole or primary basis for determining academic dishonesty. Output from these tools is not considered definitive evidence of AI misuse and may not be used independently to assign grade penalties.
- **Procedure for Review:** When academic dishonesty is suspected, educators must use professional judgment, review student work over time, and engage in direct student

conversation. If inappropriate AI use is identified, educators must follow the [BPS Code of Conduct](#). In accordance with [Superintendent Circular SUP-5](#), students must be given an opportunity to explain their thinking, parents/guardians must be notified, and educators must document concerns, evidence, and outcomes as part of a consistent and transparent process. If a school includes AI usage within their school-based rules, there must be an allowance for a hearing to address any suspected academic dishonesty, consistent with the BPS Code of Conduct procedures.

Use of AI Notetakers

The use of third-party AI tools for recording or transcribing virtual meetings is prohibited unless they are District-approved tools and active consent is obtained from all participants.

IV. Prohibited Uses of AI

The following uses of AI are prohibited for all members of the BPS community, including staff and students. The use of AI to harm, harass, or damage the reputation of others is strictly prohibited. This includes but is not limited to:

- Creation, distribution, or use of AI-generated audio, video, or images, including deepfakes or manipulated content, that clone or falsely depict real individuals without their knowledge and explicit consent.
- Use of AI tools to generate harmful, threatening, violent, or inappropriate content.

For more information about bullying, read [BPS Superintendent Circular SSS-18 Bullying Prevention and Intervention Plan](#) and section 14.9 of the [BPS Code of Conduct](#).

AI-Generated Harm and Deepfake Response

[In alignment with Massachusetts state guidance](#), BPS will respond to incidents involving AI-generated harm, including deepfakes by:

- Promptly investigating all reports involving students or staff.
- Taking immediate steps to stop the distribution of harmful content and preserve relevant evidence.
- Providing appropriate support to impacted students, including social-emotional and counseling resources.
- Addressing incidents in accordance with the BPS Code of Conduct, Bullying Prevention policies, and applicable legal requirements.

School leaders are responsible for ensuring a timely response, documentation, and notify BPS Safety Services in all matters.

Violations of this policy will be addressed and may result in disciplinary action in alignment with the BPS Code of Conduct, Acceptable Use Policy, and applicable staff policies.

V. Use of AI by Students

AI can support student learning when used appropriately and responsibly. Expectations for student use will be developmentally appropriate and guided by teachers.

Students must:

- Follow district, school, and classroom expectations for AI use.
- Only use approved AI tools when directed by a teacher.
- Not use AI tools to replace their own critical thinking, learning, skill building, and effort.
- Never enter any personal or confidential information into AI tools.

- Verify the accuracy of AI-generated content.
- Properly cite or disclose AI use as required by their teacher or school.
- Use AI responsibly and must not engage in cyberbullying, harassment, or harm to others, including the creation of AI-generated content intended to mislead, embarrass, or damage the reputation of others.

For information about academic misconduct, read section 14.2 of the [BPS Code of Conduct](#).

Age-Appropriate Use

AI use will be differentiated by grade level, with defined expectations and guidance for elementary and secondary students and with increasing access and responsibility as students progress.

Assessments

The use of AI during quizzes, tests, or projects that are assessed is prohibited unless explicitly authorized by the teacher.

VI. Family Engagement

Families will be provided with information that supports them with:

- Understanding student data privacy protections, district safeguards, and responsible data sharing practices.
- Reinforcing ethical, responsible, and academically honest AI use at home, including appropriate attribution and boundaries.
- Working with their children to critically evaluate AI-generated content for accuracy, credibility, and potential misinformation.
- Access to district-provided resources or training to build understanding of AI tools and their appropriate use.

VII. Policy Review and Updates

This policy will be reviewed annually and updated to reflect evolving technology, legal requirements, and district priorities. BPS will communicate updates to stakeholders and privacy guidance to support implementation as AI tools and use cases continue to develop.

VIII. Appendix: [Reference Circulars](#)

- OIIT-01/02/03: Technology Governance and Purchasing
- ODA-03: Student Data Privacy
- SSS-18: Bullying Prevention and Intervention
- SUP-05: Code of Conduct & Academic Integrity
- ODA-02: Test Security and Ethics
- FIN-07: Purchasing Guidelines
- HRS PM Series: Staff Evaluation and Personnel Records
- CAO-08: [BPS Grading Policy](#)

IX: Glossary of Terms

Artificial Intelligence (AI): Technology that can perform tasks that usually require human thinking, such as writing, analyzing information, or making predictions.

AI Detection Tools: Software designed to determine whether content was generated by artificial intelligence. These tools are known to have limitations in accuracy and may produce false or biased results.

AI Literacy: The ability to understand how AI works, evaluate its outputs critically, recognize its limitations and risks, and use it responsibly and effectively.

Approved AI Tools: AI tools that have been reviewed and authorized by BPS through its Privacy Impact Assessment and governance process and are included on the District's published list of approved tools.

Bias: When an AI system produces results that are unfair or inaccurate for certain people or groups.

Data Breach: A security incident where sensitive, confidential, or protected information is accessed, stolen, or used by an unauthorized party. These incidents involve the loss of control or exposure of personal (PII), financial, or health data. Breaches can be intentional or accidental.

Deepfake: AI-generated or manipulated images, videos, or audio that falsely show a real person doing something they did not, often in a way that is misleading, harmful, or deceptive.

Generative AI (GenAI): AI that can create new content, such as text, images, audio, and code.

Hallucinations: When an AI system gives false or misleading information and presents it as if it were true.

Large Language Model (LLM): A type of AI that is trained on large amounts of text and can generate human-like writing.

Misinformation: False or inaccurate information that can mislead people.

Overreliance: Depending too much on AI tools, which may lead to unrealistic expectations of AI capabilities and hinder the development of critical thinking and other essential skills.

Personally Identifiable Information (PII): Information that can be used to identify a person, such as name, student ID, address, date of birth, or records such as Individual Education Plans (IEPs), 504 Plans, and health information.

Plagiarism: Presenting someone else's work or ideas as one's own without giving proper credit.

Shadow AI: Using AI tools without the knowledge or approval of the District, especially when using for school or work-related purposes.

Training Data: The data used to train an AI system, which influences how it generates outputs and may introduce bias or limitations.