

PLEDGE TO PROTECT HUMAN-CENTERED EDUCATION

Our public schools are a public good. They are a key community institution where professional educators, governed by democratically elected officials, educate and socialize our youth to thrive in the present and flourish in the future.

Education is a human right. Privacy is a human right. Accordingly, both are recognized and supported by a body of state, national, and international law. Public schools have a duty to protect children's education and their private data—from commercial exploitation and other harms that undermine their safety, future opportunities, and personal autonomy.

Nurturing all children's agency, knowledge, and creativity is paramount to their educational development, and learning is fundamentally a social, relational activity. No advance in technology can or should replace the interaction with peers and professional educators in our schools.

In order to affirm and protect human-centered education in Chicago Public Schools, we commit to the following actions:

1) Enact a three-year moratorium on generative AI use

The Board of Education shall enact a three-year moratorium on the use of generative artificial intelligence in our public schools, including the use of Google's Gemini by high school students (rollout currently scheduled for the 2026-2027 school year.) The moratorium will pause any existing uses of such technology, including those embedded in curricula, and prohibit new contracts for such products. The Board shall then establish clear policy and detailed procedures for an approval process after gathering public input from parents, students, educators, researchers, and privacy experts on how the negative effects of generative AI on student learning, student privacy, and the environment will be prevented.

2) Appoint a Chief Privacy Officer

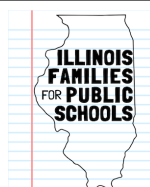
The Board of Education shall establish a Chief Privacy Officer who will report directly to the Chief Executive Officer/Superintendent. The CPO shall be an expert in student data privacy law and practices. The CPO shall be responsible for developing, implementing, and enforcing district privacy policy, based on federal and state law as well as best practices to ensure that student privacy is fully protected at all times. This will include communicating with families who have concerns and questions about their child's personal data. The CPO shall be provided with the resources required to carry out these responsibilities.

3) Limit screen time in all grades

The Board of Education shall establish a districtwide policy setting time limits on digital device use appropriate to the educational, developmental, and health needs of students at each grade level, including a ban on 1:1 digital device use before third grade.

4) Prohibit collection of biometric information

The Board of Education shall prohibit any collection and processing of biometric information unless it is required to fulfill the right of access to education under state and federal law for students with disabilities.



WHY WE MUST PROTECT HUMAN-CENTERED EDUCATION IN CPS

Education is fundamentally a human right and is best achieved through human relationships. The purpose of our public schools is to fulfill the public good of nurturing and educating all children to take on the complexity of adulthood in a 21st century, pluralistic democracy. Chicago Public Schools' stated [core values and graduate profile](#) are realized through the dedicated work of educators in concert with students, families, and communities.

Unproven, expensive, exploitative, and privacy-invasive technologies are in use across the district, sometimes in violation of CPS' own policies and state law. Furthermore, the commercial tech industry is currently pushing to embed and expand the use of generative artificial intelligence (GenAI) software in schools. It is time for a critical examination of the damage resulting from the overuse and misuse of digital technology in our schools.

The Board of Education must take these four key, value-aligned steps to commit to a human-centered education for all students.

Moratorium on GenAI: The known and potential harms of GenAI necessitate that CPS immediately protect students' educational experience and the privacy of their personal data to ensure it is not used against them.

Research shows [the harm to students' cognitive development, mental health](#), and [the physical environment](#), among other negative impacts, of GenAI. In January, the [Brookings Institute concluded](#) based on an extensive investigation that "we find that at this point in its trajectory, the risks of utilizing generative AI in children's education overshadow its benefits." In April, more than 260 organizations and experts [issued a statement](#) calling for "a five-year pause on generative AI products for students in preK-12 schools."

Currently, there is no transparency about the use of AI, including GenAI, in CPS. Families have no information about what software and sites incorporate frontier AI models; how their child's personal data and school work is being processed by AI; nor whether AI models or GenAI tools are used to make decisions about

their child's education. The [CPS Guidebook on AI](#) places the burden of mitigating the harms of GenAI on staff members as individuals—including protecting privacy, avoiding misinformation, lessening environmental harms, evaluating violations of intellectual property, and mitigating algorithmic bias.

In the absence of state and federal legislation that adequately protects students from the negative impacts of GenAI, it is the district's duty to act. **Instead of continuing to subject students to experimental technology, the district must create and implement policies that would evaluate the pedagogical, privacy, and societal impact of AI software, sites, and services before any such tech is used.**

The Board should learn from its [2016 decision to require computer science for all graduates](#) and exercise patient deliberation with respect to GenAI. At the time, Mayor Rahm Emanuel argued, "computer science...will ensure that our graduates...can compete for the jobs of the future," but a decade later, [entry-level positions](#) in the field are declining rapidly. As technology evolves quickly and high-quality independent research about its impact lags, the prudent decision is to investigate and critically assess AI tools before committing limited resources, including district funds as well as teacher and student time, to these programs.

While this pledge point focuses on GenAI specifically, district policies and procedures should be designed to analyze [the impact and proven value of any tech program before it is deployed in our schools or assigned to our students—especially those that process their personal data](#).

Chief Privacy Officer: Schools now collect, process, and hold, directly or via contractors, a large quantity of incredibly sensitive digital data pertaining to every CPS student. However, childhood is a time of growth, experimentation, and development. The mistakes and challenges of childhood should not be collected as part of a digital dossier that follows young people into adulthood and hampers their future well-being and success.

CPS continues to allow vendors and other third parties to violate its own policies and contracts,

along with state and federal privacy laws. Currently, the responsibility for protecting student data is diffused across many roles and departments. [Major breaches happen far too frequently](#). The [public reporting](#) about student data collection, processing, and disclosure is incomplete, with many vendors, as well as data sharing agreements, missing entirely. Others that are posted lack key information required under state law.

Parents, students, and staff need a [Chief Privacy Officer, a designated, executive-level officer](#), who they can rely on to address concerns about data privacy, monitor compliance, and rigorously enforce policy. **The CPO's highest priority duty will be to ensure that students are not sacrificing their personal data, educational records, and intellectual property in order to obtain an education.** The CPO must regularly and actively solicit and respond to input on how the district is protecting student privacy, including meeting with families.

New York City's [public schools have a CPO](#), as do many other districts in New York State, as well as the [US Department of Education](#), the [NY State Education Department](#), [South Carolina State Board of Education](#), among others. Los Angeles USD has a dedicated [Data Privacy, Analysis, and Reporting Branch](#).

Screen time limits: Despite the [negative academic, social, and health effects of the overuse of 1:1 digital devices at every grade level](#), their dominance has only increased over the past two decades in CPS, with the fastest growth in the last six years. While digital technology has expanded access to human knowledge, children best learn in a classroom environment where they can interact with each other and with their teachers. **Early childhood education (birth to age 8) does not require the use of screens, and a full ban before third grade should be instituted. Digital device usage from grades 3-12 must be based on a rigorous analysis after consulting the research and gaining input from stakeholder groups.** Exceptions to limits on device use must be made for technology that enhances accessibility for students with disabilities if such methods are cited in their IEPs or 504 plans and based on the available research.

Biometric information ban: While all personal information needs protection from security and privacy threats and commercial exploitation, an individual's biometric information is irreplaceable and irrecoverable once it is shared. **Collection of biometric information—whether face scans, fingerprints, voiceprints, or other biometrics—should only be allowed when strictly necessary to implement the requirements of IEP or 504 plans for students with disabilities**, i.e. if there is no suitable substitute that allows for a student's access to an appropriate education to be met otherwise. This exception should require voluntary, informed written consent from the student's parent or guardian, and such data must be protected from further disclosure with the most rigorous methods.

References

- [AI Moratorium for NYC schools petition](#) (2026)
- [The Carbon and Water Footprints of Data Centers and What This Could Mean for Artificial Intelligence](#). (2026) *ScienceDirect*
- [Chief Privacy Officers: Who They Are and Why Education Leaders Need Them](#) (2019) Center for Democracy and Technology
- [Coalition of Organizations and Experts Calls for Pause on Generative AI in PreK-12 schools](#). Fairplay
- [Facial Recognition Technology in Schools: Critical Questions and Concerns](#). (2020) *Learning, Media and Technology*
- [Fit for Purpose? How Today's Commercial Digital Platforms Subvert Key Goals of Public Education](#). (2025) National Education Policy Center
- [A New Direction for Students in an AI World: Prosper, Prepare, Protect](#). (2026) Brookings Institute
- [Parent Coalition for Student Privacy Parent Toolkit](#) (2017)
- [Screen Time Limits Call for Nuance. Disability Advocates Say](#). (2026) *K-12 Dive*
- [Time for a Pause: Without Effective Public Oversight, AI in Schools Will Do More Harm Than Good](#). (2024) National Education Policy Center
- [Use of Biometric Identifying Technology in Schools](#) (2023) New York State Office of Information Technology Services
- [Using Technology with Intention: Establishing Guidelines for Student Screen Time](#) (Resolution # 048-25/26) Los Angeles United School District