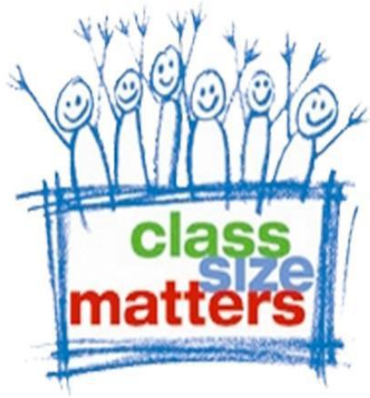


The need to strengthen student privacy against data breaches, commercial exploitation & the expansion of AI



Parent Coalition for Student Privacy

Presentation to Parent Action Conference
Leonie Haimson, Parent Coalition for Student Privacy
June 7, 2025

NYS Ed Law §2-d: fairly strong student privacy law passed in 2014 result of inBloom controversy

- inBloom Inc. launched in February 2013 with more than \$100M in Gates funds, designed to collect personal data of millions of public-school students in 9 states and districts, and share it with for-profit vendors to build their ed tech tools around.
- Many parents, educators and district leaders protested & every participating state and district pulled out of inBloom. NY was last when Legislature passed a bill requiring this in March 2014. In April 2014, inBloom closed its doors.
- NY Legislature also passed new privacy law Ed Law §2-d; after years of delay, SED finalized regs for the law in January 2020. Covers all public schools, charters & certain Pre-K and non-public schools, [described here](#).
- In June 2014, the Parent Coalition for Student Privacy established because parents nationwide realized that federal privacy laws not strong enough. More than 100 new state student privacy laws were soon passed.
- Yet DOE has never fully complied with Ed Law §2-d and recently revised Chancellors regs to weaken its privacy protections.



How does Ed Law §2-d protect student privacy ?

- **Ed Law § 2-d:** Every school vendor with access to student PII must have contract addendum that establishes how that data will be protected & that doc must be posted on the district website
- PII must be encrypted at all times at high level of security, as specified by National Institute for Standards and Technology Framework Cybersecurity version 1.1
- Vendor access to PII must be minimized & deleted when no longer needed to carry out contracted services
- Parents must be told how they can access their children's data held by DOE or the vendor & challenge it if inaccurate
- Parents must be notified within 60 days of the district becoming aware of a breach
- Student PII cannot be sold or used for marketing or commercial purposes --including to improve products or create new ones
- Parents can file complaints to the district and/or State if their children's data has been improperly disclosed
- Vendors can be penalized financially if they don't comply with law &/or barred from future contracts



What is student personally identifiable information or “PII” ?

- A student’s name and the name of their parents or other family members;
- Their contact information, including phone, email, home address or IP address, based on their Wi-Fi network or router;
- Personal identifiers, such as social security number, student ID number, or biometric records;
- Other indirect identifiers, like date of birth, place of birth, or mother's maiden name;
- School-based education and health records, whether in the form of printed documents, photos, film, audio or video files that could identify them.
- Any other information, including school, ethnicity, grade, or class, that alone or in combination could identify the student with reasonable certainty.
- All this data can be shared with vendors and other third parties according to Ed Law 2d, if they are performing services for schools, or for research purposes, as long as they are under the direct control of the school
- This usually means a written agreement or contract explaining how PII will be collected and used only for that specific purpose and protected from further disclosure.

What's the harm of breaches or disclosing student PII without restrictions?

- Student PII is very valuable for identity theft as most minors do not already have credit ratings
- Excessive monitoring of student's internet use by schools can be devastating to their sense of individual freedom
- Their data can also be used by schools for racial profiling and other discriminatory actions
- Student PII can be used by ad tech and social media companies for marketing, bombarding them with ads, & even undermining their mental health, as noted in recent NYC & state lawsuits vs these companies
- Negative info about a student can affect their future opportunities, including jobs, college admission, medical insurance, etc.
- Student data can also be used to threaten their safety, leading to cyberbullying, sexual harassment, abuse, abduction or deportation



Despite Ed Law 2-d mandates, DOE's lax security measures have led to repeated breaches

- *As of Dec. 2024, DOE had agreements with at least 523 ed tech companies, 55 Related Service Providers, and 50 Research groups to allow them to access student PII, which we know as they had privacy addendums on DOE site*
- Yet many companies w/access to student PII have **no privacy agreements** posted on DOE website– including some that suffered breaches & many of the privacy agreements that ARE posted do NOT fully align with law
- Example: In Jan. 2022 , Illuminate breach exposed personal data of more than million current and former NYC students, including dates of birth, ethnicity, academic records, special ed and/or free lunch status --including thousands of former students.
- When DOE privacy agreement w/Illuminate subsequently posted, it hinted that PII was NOT always encrypted. Though security audits were offered, no indication that DOE ever asked for them
- May 2023, Movelt breach released PII for 45,000 students, in addition to DOE staff and related service providers – with no privacy addendum or contract ever posted.

Case study: PowerSchool breach

- Jan. 9, 2025; PowerSchool announced that in late December, their Student Info System had been hacked, exposing student PII from many districts and schools nationwide, and began informing them of the breach
- Among data released, depending on school and district, were student names, contact info, date of birth, grades, test scores, special education status, mental health details, disciplinary notes, parental restraining orders and more – as well as teacher PII in some districts.
- DOE initially told reporters that no NYC schools were affected though this wasn't true: instead, data had breached from *Fordham HS for the Arts*, *Westchester Square Academy*, *Long Island City High School*, and *Lower East Side Prep*.
- On Feb. 3, 2025, we were alerted by NYSED that DOE told them these NYC schools that enroll about 3,000 students were likely affected; yet DOE still refused to confirm this to reporters

PowerSchool breach (Part II)

- As of Feb. 26, 2025, 2 months after the breach, DOE had still said nothing publicly or on its website, despite [NYSED guidance](#) this should be done “***to capture as wide an audience as possible***” especially as former students may also have been affected.
- DOE only alerted current families of the breach the first week of April, which violate the [Ed Law 2D regulations](#) which require notification w/in 60 calendar days– and still have not posted the names of the schools or that former students also had their info breached on the DOE website.
- In early May, it was widely reported that ransomware criminals had reached out to schools & districts asking for ransom to be paid or else they would release the data; nothing about this 2nd wave of attacks either has been mentioned by DOE publicly or on its website.
- More than 20 lawsuits have been launched vs PowerSchool nationwide for not taking the most basic security protections against hacking, including multiple authentication – yet still DOE allows schools to use 16 other data-hungry PowerSchool products.

STILL DOE authorizes schools to use 16 other data hungry PowerSchool products – including Naviance that commercializes student data



- Naviance, a college/career planning program, is used in many NYC HS, which collects a huge amount of student PII & [sends targeted ads](#) to students, disguised as objective recommendations, in violation of State law. The company has been shown to allow colleges to discriminate by targeting ads to white students only.
- Other PowerSchool programs DOE allows NYC schools to use that collect student PII: *Enrollment*, *Enrollment Express*, *Performance Matters Advanced Reporting*; *Performance Matters Assessment*; and *PowerSchool SIS*
- Student and teacher data: *Unified Talent Employee Records*; *Unified Classroom Schoolology Learning*; *Unified Classroom Curriculum and Instruction*
- Special education, SEL and behavior data: *Unified Classroom Special Programs*; *Unified Classroom Behavior Support*, plus six more!
- ***None of these programs should be trusted given PowerSchool sloppy privacy practices and inherent weakness of the DOE contract.***

In any case, DOE's privacy agreement with PowerSchool is defective and does NOT conform to law.

- PowerSchool is now facing numerous state lawsuits for lax privacy practices including failure to use double authentication – standard procedure to protect security of PII.
- But as we pointed out months ago, PowerSchool's privacy agreement w/DOE says the company will *“Review data security and privacy policy and practices to ensure they are in conformance with all applicable federal, state, and local laws & the terms of this DSPP [Data Security Privacy Plan]....*
- ... *In the event Processor's policy and practices are not in conformance, Processor will implement commercially reasonable efforts to ensure such compliance.”*
- In other words, PowerSchool **will only comply with federal and state privacy laws when it doesn't unduly affect their bottom line.**

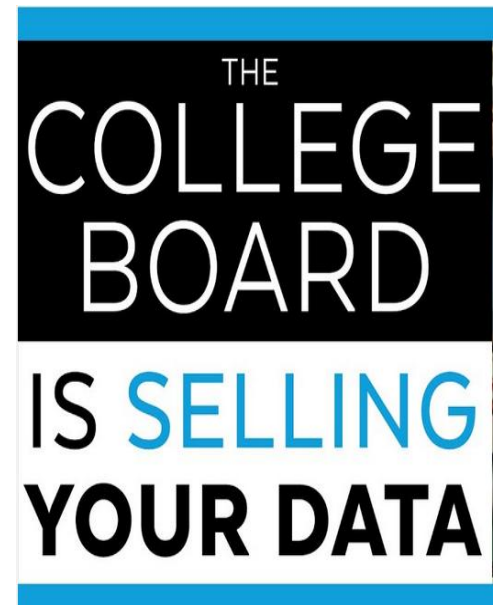
State Comptroller found DOE had inadequate breach notification



- [State Comptroller](#) reported that 80% of DOE cybersecurity incident reports lacked enough detail to tell if students and teachers were informed within the legally required 60-day timeline.
- In more than half of incidents, NYC DOE blew past the legal deadline to notify NYSED of the problem.
- And yet NYC DOE still is expanding use of ed tech and online learning, including risky AI programs, multiplying risk of data breaches and misuse of student data – without necessary guardrails & now proposing to weaken Chancellor A-820 privacy regs.

College Board – a known violator of state student privacy law

- For years, College Board made more than \$100 million annually selling personal student data collected from students during testing in school and when they sign up for accounts.
- This included student names, addresses, race/ethnicity, grades, income and test score ranges, even though this sale violates student privacy law in NY since 2014
- We protested this practice to DOE & they did nothing to stop it.
- Finally, in February 2024, NY Attorney General negotiated a consent agreement with College Board & they agreed to stop this practice and pay a fine of \$750,000.
- But we have no idea how this will be enforced or monitored – especially as ***DOE had no current contract with College Board since June 2023*** – even as hundreds of thousands of NYC HS students took AP, PSAT and SAT exams in 2023-2024 in their school & DOE paid them millions for those tests!



College Board – another weak DOE privacy agreement

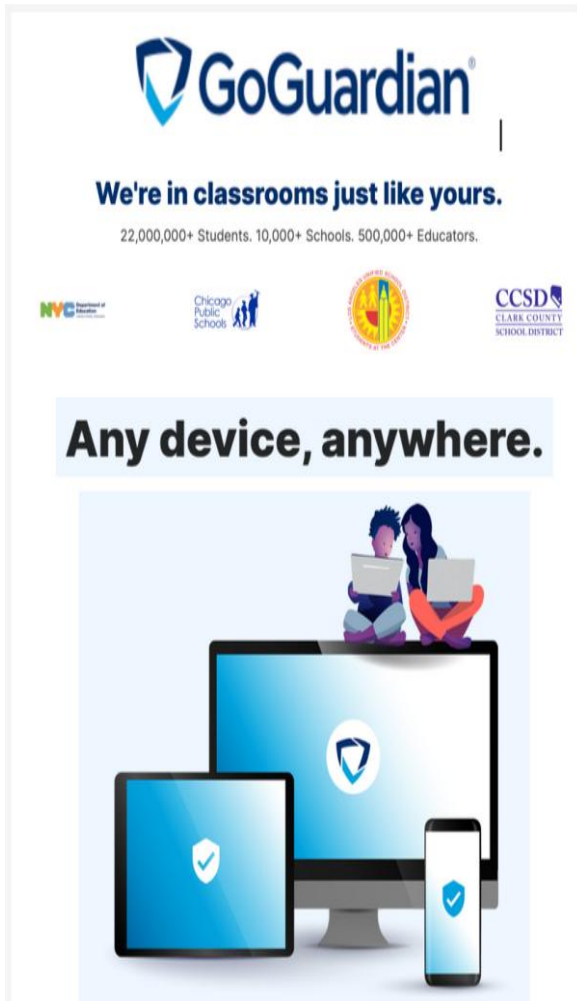
- CB Privacy agreement posted on DOE website says the company & its subcontractors will NOT encrypt student data “***where data cannot reasonably be encrypted***”
- Also says it will delete the data only “***when all NYC DOE schools and/or offices cease using College Board’s products/services***”.
- For the SAT/PSAT, the PBOR contains ***no specific date or time*** when the data will be deleted – both are contrary to the law.
- Recently, bill has been introduced to create a loophole in the Ed Law 2D to allow the College Board to continue monetizing student data
- A9967/ S9597 would allow CB to send targeted ads to student phones, paid for by colleges and other companies, based on their data, including their grades, test scores, race and ethnicity – and yet CB is doing this anyway already in violation of the law!

Expansion of AI likely to further undermine student privacy



- DOE encouraging principals and teachers to expand use of AI without guidance, though most Generative AI programs harvest personal data to improve their products as pointed out [Center for Artificial Intelligence and Digital Policy FTC complaint](#).
- Open AI [admits](#) that “Chat **GPT-4 has the potential to be used ...to identify private individuals when augmented with outside data**” and that its use could “**reinforce & reproduce specific biases & worldviews, including harmful stereotypical & demeaning associations for certain marginalized groups.**”
- Their official policy says no child under 13 should be using Chat GPT, and no student aged 13-17 without parent consent. Other AI programs have similar age-linked restrictions which are ignored by many families and schools.
- Yet DOE has put out NO guidance or guardrails to ensure that student data is not monetized or abused via use of AI in classrooms and schools.
- HMH Writeable and Amira are both HMH products that schools are encouraged to use, even though they use AI and collect student data for “**Product improvement**” which violates state law

Some NYC schools also surveille students without alerting parents



The advertisement for GoGuardian features the company logo at the top left. Below it, the text reads "We're in classrooms just like yours." followed by "22,000,000+ Students. 10,000+ Schools. 500,000+ Educators." Below this text are four logos: NY State Department of Education, Chicago Public Schools, a circular logo with a torch, and CCSD Clark County School District. At the bottom, the slogan "Any device, anywhere." is displayed above an illustration of a desktop monitor, a laptop, and a smartphone, all showing the GoGuardian shield logo. Two stylized figures are sitting on top of the monitor, looking at a laptop.

- Oct. 2021, Bloomberg News [reported](#) that NYC DOE signed a contract with GoGuardian that sells surveillance/spyware installed on computers used by students and that could spy into their homes without their knowledge if not properly configured.
- When a PEP member asked to see this contract in Nov. 2021, DOE said there was none, but that they were ***“able to Centrally make this product available to all schools through the Enterprise G-Suite/Google Workspace license at no cost to school nor to families”***
- More recently, the DOE posted a GoGuardian privacy agreement online, for a contract that they say started in Aug. 2021, but it lacks sufficient detail and says that it lapsed in August 2024.
- According to GoGuardian, best practice is to inform parents beforehand that this program is being used and installed on their children’s computers, and allow for parent opt out, but we do not know if this has been done in NYC schools.

DOE revisions to Chancellor's privacy regs!

- Chancellors reg A-820 on student privacy hadn't been updated since 2009, but new version was approved in May 2025
- Example: DOE & individual schools now authorized to share a huge range of very sensitive PII w/ non-school vendors & w/anyone they please, including student names, emails, home address, phone #s, photos,, & more, by calling this "Directory Information" w/o any protections of Ed Law 2D & only with unreliable parent opt out.
- The only data exempted from disclosure are test scores, grades, demographic & special education info

NYC DOE's definition of DI is contrary to DOE own advice and NYSED guidance

- These revisions ignore DOE [statement on its website](#) that ***home addresses, telephone numbers are too sensitive to be considered Directory Information.***
- [NY Department of State](#) warns that identity theft of minors can occur with only a few items of personal data, which could seriously damage their prospects since crimes can go undetected for years:
- *“The damage caused by child identity theft can vary from a single fraudulent bill in collections to a foreclosed mortgage.*
- Disclosure of this data could also lead to commercial exploitation, sexual victimization, cyber bullying, abduction, and/or deportation efforts.
- The only significant improvement made by DOE after discussions with the Chancellor's Data Privacy Working Group was to require written agreements with the companies and individuals receiving the data with privacy and security protections – but as we have seen, this is often ignored by the third party and rarely enforced by DOE.

Health & medical records insufficiently protected

- DOE also proposes that student health & medical records at schools would NOT be protected by Ed Law 2d if made by NYC Dept of Health staff or other officials, at school-based health & mental health clinics.
- [Yet federal guidance](#) says: *"Health records that directly relate to students and are maintained by a health care provider, such as a third-party contractor...would qualify as education records subject to FERPA regardless of whether the health care provider is employed by the school."* State law does not exempt records kept at schools from its protection.
- We have already seen how student data can be abused when it is NOT protected by Ed Law 2D, as in the NYC Dept. of Health contract with Talkspace , which has allowed sensitive mental health data of NYC teens using their services to be exploited for commercial purposes and shared with social media companies.

Already, DOE also shares student/parent info with charter schools to help them recruit students

- For years, DOE claimed this is legal as they only indirectly provide family addresses etc. through the DOE mailing house
- Yet many parents report being barraged by phone calls from charter schools as well
- While DOE claims parents can opt out of these mailings, but even after parents do so, many say they are still inundated with mailers and phone calls – showing how fallible the opt out process is
- NYC only district in country that provides this personal student info voluntarily to charter schools for recruiting
- Now charter schools will be eligible to obtain even more info- including students who made honor rolls, teams, etc. and recruit them directly through their emails and phones.



Charter School Informational Mailing Notice and Opt-Out Form

The New York City Department of Education (DOE) ensures you have access to important information about City schools, including charter schools.

The DOE shares students' names, parents' names, mailing address, zip code, and grade level with a vendor named Vanguard. Vanguard then mails school information to families. Charter schools also use this vendor to mail informational materials on their behalf. Vanguard is not permitted to sell the information, give it to others, or use it for any purpose other than for the charter school informational mailings. Vanguard is prohibited from sharing this information with charter schools or charter school organizations. Your information is never directly disclosed to a charter school or charter organization.

How to Stop Receiving Charter School Informational Mailings

If you wish to receive these mailings, you do not need to do anything. If you do not wish to receive charter school informational mail, please fill out and submit the survey **no later than October 31**. If you miss this deadline, you can submit the survey by **January 15** to stop receiving the mailings after March. You will need to submit a survey for each of your children. If your child is age 18 or older, they must complete the survey or form themselves.

Please note: you will need your child's unique student ID number (OSIS number) in order to complete this survey. If you do not know your child's OSIS number, contact your school's front office or parent coordinator for assistance. To find contact information for your child's school, use [Find a School](#).

Parent Name *

Our work on student privacy continues – do you want to be involved?

- We also be reaching out to parents directly and through the CECs on how they can opt out of these disclosures to non-school vendors in the fall. Sign up for our CSM list serve at <https://classsizematters.org/newsletters/>
- Data Privacy Working Group expected to keep working & tackle AI in schools as well as need for enhanced data security protections. We will push for public feedback sessions to hear from parents and teachers their concerns.
- We are about to put out alert about the US House bill that includes a provision that no state or locality could regulate on the use of AI for ten years – a bill that the US Senate is taking up next week. Meanwhile NY [Senate Bill S7599A](#) would require all govt agencies including school districts to produce impact & privacy assessments on use of AI & automated decision-making.
- If you want to file a privacy complaint and/or be put on our mailing list for further updates on the privacy issue, email us at info@studentprivacymatters.org