

How NYC public school parents can better protect their children's privacy

Leonie Haimson

Nov. 10, 2026

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

- Every school vendor with access to student personal info (PII) must have contract showing how data will be protected & a privacy addendum to contract must be posted on district website
- PII must be encrypted at all times at high level of security
- Vendor access to PII must be minimized & data deleted when no longer needed to carry out contracted services
- Parents must be told how to access their children's data held by vendors & challenge it if inaccurate
- 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 NYS if their children's data was improperly disclosed & have complaints responded to within 60 days & notified of breaches within 60 days
- Vendors can be penalized financially if they do not comply with law &/or barred from future contracts
- **Yet NONE of these provisions have been consistently implemented by DOE.**
- More complete list of parent rights under the law here.

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
- Their data can also be used for racial profiling, deportation, 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
- 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



State Comptroller found DOE had inadequate breach notification



- State Comptroller audit in April 2026 showed DOE had inadequate data privacy protections & failed to comply with NIST security standards required by law.
- Between Jan. 2023- Feb. 2025, suffered at least 141 breaches & reported 48% of them past legal deadline to State Ed; 11% late to affected families.
- In many cases, DOE did not even know which schools used which products or which personal student data these products collected or breached
- Fewer than 75% of employees had completed required privacy training
- Audit found other critical weaknesses in technical controls that need to be corrected.
- DOE rejected most of recommendations or said they already had made all necessary changes.

Continuing issues with DOE's expansive data sharing & lax oversight to ensure privacy

- Over time, DOE has made agreements with at least 523 ed tech companies, 95 Related Service Providers, and 100 Research groups with access to student PII, with posted privacy addendums on DOE site
- Unknown number of other vendors w/access to NYC student PII have **no posted privacy agreements**–including some that suffered breaches, like MoveIt, that released info from 45,000 students in May 2023, in addition to staff and related service providers –
- Several of the DOE privacy agreements that ARE posted do NOT fully align with law
  - In Jan. 2022 , Illuminate breach exposed personal data of more than million current and former NYC students, yet the privacy agreement was never posted before the breach & when it was, it suggested that PII was NOT always encrypted.
  - Though security audits were required, no indication that DOE ever asked for them.
  - Though data deletion required by law, DOE never asked for deletion leading to MANY thousands of former NYC students who'd long left the system, but whose data breached anyway
  - 380,000 NYC families were not informed until May 2024, more than 2 years after the breach

Breach of PowerSchool data

- Jan. 9, 2025, PowerSchool announced that its Student Info System (SIS) had been hacked by cybercriminals, resulting in largest student data breach in US history, including millions of students nationwide & thousands of current & former NYC students.

- Among data breached: 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 only confirmed to families that their kids had their data breached week of April 1 after legal deadline

- PowerSchool had not employed basic security measures & now has two different major class action lawsuits launched against its products, plus recently settled a third lawsuit for $17.25 million regarding its Naviance product.

- Yet DOE has now re-approved four PowerSchool products for use in schools, including those named in the lawsuits and in court settlement-their SIS, Naviance, Schoology, & Kinvolved/School Messenger

Expansion of Gen AI further undermines student privacy

- Generative AI programs generally data-mine user personal information and use if for product improvement., yet we've heard of teachers assigning off-the-shelf AI products to students., like Chat GPT.
- Open AI says in its ChatGPT Privacy Policy that "no child under 13 should be using Chat GPT, and no one age 13-17 without parent consent". Other AI programs have similar age-linked restrictions which are ignored by many schools.
- Open AI explains that "Chat ***GPT-4 has the potential to be used …to identify private individuals when augmented with outside data***"
- Open AI's own research and that of others show that its use could "***reinforce & reproduce specific biases & worldviews, including harmful stereotypical & demeaning associations for certain marginalized groups***."
- Yet AI companies are desperate to collect and incorporate more personal information from students and others, as they predict a shortage of high-quality data in near future to improve their products and to use for other profitable purposes

DOE revisions to Chancellor's privacy regs

- Despite need for enhanced privacy protections, Chancellor's regulation A-820 was revised and weakened in May 2025

- The revisions allow DOE & individual schools to disclose sensitive student information w/any company or vendor even if they do not provide educational services to schools, by calling this "**Directory Information**" (DI) with a parent opt out process to prevent this.

- Among the personal data that can be disclosed are *student names, emails, home address, phone #s, photos, participation in honors programs, arts, theater, sports & more*

- Only data exempted from disclosure under these regs are student SSN, test scores, disciplinary data, grades, attendance, demographic info & special education and multilingual status

- We will tell you how to opt out of these DI disclosures that DOE will be making

DOE Directory Info disclosures that parents are allowed to opt out of

- **Kids Rise college saving account (***K-4th grades, or higher if parents are not opted out before)*
- **Armed forces & colleges** (*11th and 12th grades)*
- **National Student Clearinghouse (***high school students***)**
- **Charter school mailings** (3*K- 11 grades*)
- You can use our **Directory Info opt out form**. Though unofficial, parents should fill it out & submit to your schools ASAP.
- Also, fill out separate online forms ASAP; **instructions and links here.** In some cases, official deadlines have recently lapsed but do this anyway if you want to opt out of these disclosures.
- **Schools can make separate DI data disclosures under this policy, and many do.**

What disclosures does DOE say parents cannot opt out of?

- DOE says parents can't opt out of disclosures to companies providing educational or operational services & with whom they have privacy agreements

- This based on "school official" and/or "audit &/or evaluation" exceptions to FERPA, federal law weakened through rewriting regs in 2008 & 2011 to encourage ed tech expansion & data tracking for "accountability"

- 107 ed tech products were recently re-approved by DOE for school use according to list provided to administrators as of Nov. 2, 2026 – 34 of them only teacher facing.

- You should check to see if your child has been assigned to use any products **not** on this list and if so, let us know at info@studentprivacymatters.Org

Questions to ask your schools about data disclosure

1. Which of my child's Directory Information (DI) will be disclosed by the school and to whom? According to federal law and Chancellor's Regulation A-820, parents have the right to opt out of these disclosures. Please provide me with all opt out forms, types of student data you or DOE have designated as DI, the specific purposes of these disclosures, & the deadline to opt out.

2. Please provide me a list of other companies or third parties that will have access to my child's personal data for educational or operational purposes. According to NY Ed Law 2d, parents have the right to be informed of the names of these companies & their products and inspect the data collected within 45 days of a request.

3. *(To follow up if they are not on this list of products):* **Why is the school utilizing this program when it is not on the DOE list of approved products?**

Questions about AI use

1. **Which products assigned to students use Gen AI, if any?** (Especially relevant to parents of kids with IEPs, 504s, ELLs & many HS students, exempt from AI moratorium.)

2. **Will Google Search be turned off in student Chromebooks and other devices & in their Google school accounts as it uses AI, according to Google? If it will be turned off, when will this occur and will students be told not to use it in the meantime?**

3. **Will students be encouraged to use a privacy-protective search engine and browser instead, such as those from Duck Duck Go?**

4. **Will students be informed not to use any off-the-shelf AI products for their schoolwork, especially as these products data-mine personal data and are non-compliant with NYS privacy law?** (For example, Open AI/ChatGPT Privacy Policy says never should be used by kids under 13 & those 13-18 only with parent consent.)

5. **Which AI products will teachers use, and how will they ensure no personal student information is shared with these companies, to prevent them from redisclosing the data or harvesting it for commercial purposes?**

Questions about screen time

1. **How many hours per week will my child be assigned to spend on computers or tablets, either at school or home, and which ed tech products will they be assigned to use?**

2. **Which of these products are exempt from the DOE's recommended screen time limits of zero time for 2K-2nd grades, 30 minutes daily 3rd-5th grades, and 45 minutes daily for 6th-8th grades?**

3. **Which products or apps can I opt my child out of?**

4. (If your school has asked you to sign a computer use consent use form): **What happens if I refuse to sign it or withdraw my consent?**

5. **Will my child be assigned to watch YouTube videos, even though YouTube announced years ago that its use of student data no longer complies with the NY privacy law?**

Where can I find these questions and what should I do afterwards?

- We have a list of these questions here. ***En Español aqui.***
- If you ask some or all these questions, keep track of the date you sent the email.
- If your school fails to respond promptly, let us know so we can help if you want to file a complaint.
- If your schools does respond promptly with the names of these products, please share the list so we can keep track & help if you want to request a copy of the data they are collecting.
- ***Or we can help if you would like to contact the companies to opt out***.

This year we will help parents of kids under 13 with a new opt out strategy

- COPPA is a federal law passed in 1998, overseen by the Federal Trade Commission that gives parents the right to consent before any online product collects personal info directly from their child under 13 - or to opt out afterwards & have that data deleted.

- In 2013, FTC put out a FAQ that schools can consent on behalf of parents to collect and process this data but only if used solely for educational purposes

- Yet this FAQ doesn't have the force of law – and does not say that parents cannot opt out of this collection &/or have their child's data deleted.

- FTC repeatedly threatened to enact regulations to allow schools to agree to data disclosures of students in place of parents but has not done so

Recent encouraging actions by FTC

- In Aug. 2024, FTC filed an amicus brief in a lawsuit vs. an ed tech vendor called IXL, saying it is *"beyond doubt that COPPA and its implementing regulations do not themselves…compel parents to be bound by any agreement between schools and educational technology companies."*

- Concurring statement of FTC Commissioner Andrew Ferguson : "I see nothing in COPPA's text that limits parents' statutory right to notice and consent when their children are online at school."

- And: "***it may require website operators to obtain consent from parents even if state law otherwise authorizes schools to act on behalf of parents regarding the purchase of software.***"

- Ferguson became Chair of the FTC on January 20, 2025.

So, what strategies do we propose?

- Any parent of child under age 13 who wants to opt out of a specific ed tech program assigned to their child should email the company, copy DOE and us. (principal optional).

- The email should demand right to have their child opt out of using the program & for their data to be deleted. We will provide a sample email, prepared by an attorney.

- If the company doesn't respond within 30 days that they will honor this request, we will help parents prepare a complaint to the FTC.

- We encourage as many willing parents as possible to do this – as the more parents involved, the more likely that FTC will rule in our favor.

Other strategies for parents of students of any age

- We suspect many of the ed tech vendors use data for commercial purposes--including product improvement in violation of NY Ed Law 2D , including HMH (7 approved products), 3 AI pilot companies to be used in HS, plus Naviance, College Board, and more are suspect

- 17 approved products have no privacy posting on DOE website as required.

- Several companies admit to using student data for product improvement in their public Privacy Policy, including HMH whose privacy posting on DOE website links to webpage which says student data will be used for "*product improvement*"

- PowerSchool still has statement on DOE website saying that they will comply with federal and state privacy law only when "commercially reasonable."

Google Search – a special case

- After DOE told Google this fall they wanted AI tools like Gemini, Google AI mode, and AI Overview switched off in student devices, Google said they would also switch off Google Search, since it uses AI.

- Now Google says DOE can keep Search switched on but will not remove the AI functionality

- Google Search has had AI embedded for at least two years, & even longer has used student data for commercial purposes, including serving users ads based upon their queries.

- Lawsuit was recently filed vs. Google AI for encouraging a student to commit suicide.

- As Josh Golin of FairPlay said, "*Schools should use this opportunity not only to turn off AI, but to teach students that 'Google' isn't a verb, but the name of a surveillance and advertising company whose presence in schools has nothing to do with learning*."

- Instead, our schools should be assigning students to use a more privacy protective browser and search engine like Duck Duck Go.

Data tracking and use of ad tech/cookies

- Many ed tech products feature trackers that collect IP addresses, use cookies, & disclose data to ad and social media companies
- Recent audit by Utah State Ed board found that that 61% of ed tech apps used in their schools shared student personal data with third parties, and 36% with ad tech companies.
- NYC Dept of Health has $27M 3-year contract with Talkspace to provide online mental health services to teens, but we found via Blacklight tool they were using 15 ad trackers and 34 cookies
- These trackers shared teen personal & mental health data with Facebook, Amazon, Meta, Google, and Microsoft among others -- same social media companies that city was suing for undermining teen mental health
- After several months, we along with NYCLU and AI for Families convinced DOH to force Talkspace to remove most of these trackers.

Will you help us investigate use of adtech & other sort of data trackers?

- We used a simple tool called Blacklight on Talkspace website to identify the trackers and cookies used on their website

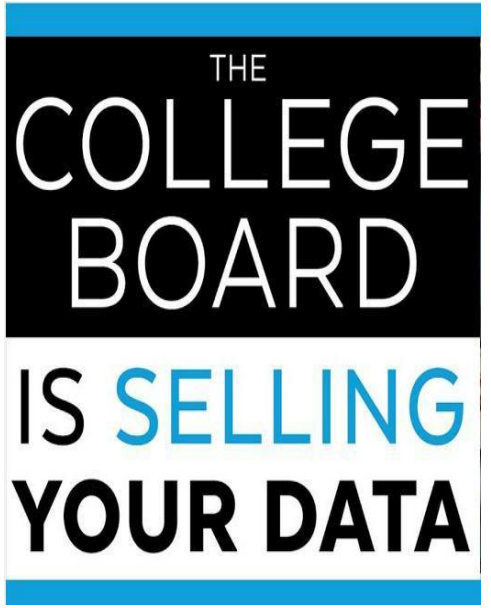
- If you are interested in seeing if your child's data is being tracked in this way, we can provide you with instructions on how to do this, & check what companies if any are collecting & sharing their data for commercial purposes

- This sort of data tracking was what led to class action lawsuit and recent $17.25 million Naviance settlement, when shown to sharing sensitive student info with ad tracking companies like Heap Inc., Google, Microsoft, and Gainsight

- Once you do, we can discuss next steps in terms of potential complaints & or legal action.

College Board – a known violator of state privacy law

- College Board made more than $100 million each year selling personal student data collected from students at school during testing when they sign up for College Board accounts for the SAT &/or AP exams.
- Data sold includes student names, addresses, race/ethnicity, grades, income and test score ranges, ***even though this sale violates student privacy law in NY since 2014***
- In February 2024, NY Attorney General negotiated a consent agreement with College Board to stop this practice and pay fine of $750,000.
- But parents report that their kids' data still being sold by College Board and/or used for targeted advertising when they sign up for a CB account – in violation of Ed Law 2D.
- If your child is in 11th or 12th grade and has signed up for a College Board account & want to help us challenge this, let us know



Legislative action

- We are planning to urge NYC Council and/or State Legislature to strengthen privacy, & places bans on AI and restrict ed tech use.

- Some relevant bills have already been proposed in these bodies, with differing strengths and weaknesses, and we expect more such bills to be proposed in the future

- If you are willing to meet with your Council Member &/or Legislator to strengthen student privacy protections and restrict AI, ed tech and screen time, please let us know

- We have a follow-up survey that we'd love youe hope you will answer, either now or after the presentation is over, about how you might like to get involved in this fight: https://forms.gle/AA891hM2xKA6vKg38

Any questions?

