



THE COUNCIL
OF
THE CITY OF NEW YORK

November 19, 2024

Dear Chancellor Melissa Aviles-Ramos:

We were encouraged to learn that the Chancellors regulations A-820 concerning student privacy would finally be updated. This was long overdue since they had not been revised since 2009. However, we urge you to significantly revise the proposed updates, to ensure personal student data cannot be disclosed by DOE or schools to outside organizations, individuals, or companies without the full protections of Education Law §2-d, unless there is parent consent.

The expansion of ed tech use in our schools has led to several large-scale data breaches of personal student information in NYC and elsewhere. There has also been increased awareness of how children's data is too often a target for predatory marketing by social media companies and the like, in ways that can undermine their mental health.

In recognition of these growing threats, in 2014 the Legislature enacted a new law to provide more rigorous student privacy protections, Education Law § 2-d.¹ Yet the proposed revisions to the Chancellors regulations would weaken existing regulations rather than strengthen them, creating serious risks to the privacy, safety, and health of NYC students.²

These regulations would authorize the Department of Education and schools to disclose a vast amount of sensitive personal student data to anyone they choose, as long as they deem this to be beneficial, *"including but not limited to: name; address; telephone number; e-mail; home address; photographs; date of birth; grade level; enrollment status; dates of enrollment; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and schools attended."*

The release of this data would be authorized with few if any of the privacy and security protections in Education Law § 2-d, and no written agreement required to prevent against breaches, redisclosures, or the misuse of the data, and no safeguards except a fallible parental opt out process.

The DOE is proposing that this vast and essentially unlimited array of personal data could be designated as "Directory Information," yet this ignores that there is no mention in Education Law §2-d of Directory Information, nor does it specify that any student personal data should be exempted from its mandated safeguards. Moreover, DOE's own website warns that student information such as *"home addresses, telephone numbers, and dates of birth [are] sensitive in nature. As such, schools are strongly encouraged not to designate this information as directory information."*³

Despite a letter from the Parent Coalition for Student Privacy pointing out many of these flaws in these proposals, and 3,000+ emails sent to Department of Education and Panel for Education Policy members

¹ <https://www.nysenate.gov/legislation/laws/EDN/2-D>

² The regulations, now revised twice but with only minor changes are posted at <https://www.schools.nyc.gov/get-involved/families/panel-for-education-policy/panel-meetings>, under the Nov. 20, 2024 meeting.

³ <https://www.schools.nyc.gov/about-us/policies/data-privacy-and-security-policies>

protesting the revisions, only minor changes have been made to the regulations, now due to be voted upon by the Panel in the coming weeks.⁴

As the NY Department of State points out, identity theft of minors can occur with only a few items of personal data such as their names and birth dates, and these crimes can go undetected for years, seriously damaging their future prospects: “*Child identity theft occurs when someone uses a minor’s personal information, such as name and birth date.... The damage caused by child identity theft can vary from a single fraudulent bill in collections to a foreclosed mortgage.*”⁵

A child’s personal data, including their photos, could also be used to threaten their physical safety and mental health, leading to predatory marketing, sexual harassment, deepfake porn or even abduction if this information fell into the wrong hands. Given the explicit plans of President-elect Donald Trump, the disclosure of this information could aid in efforts to deport migrant students, based on their hotel or shelter addresses.

We are also concerned that the proposed revisions would exempt certain student medical and mental health records maintained in schools from the full privacy and security protections of Education Law §2-d, if they were prepared by Department of Health, rather than DOE staff.⁶

Before any vote to approve these regulations, we urge you to significantly revise them, to ensure personal student data cannot be disclosed by DOE or schools to outside organizations, individuals, or companies without the full protections of Education Law §2-d, unless there is parent consent.

Thank you for your prompt attention to this urgent matter.

Sincerely,



Shekar Krishnan
Council Member – District 25



Rita Joseph
Council Member – District 40
Chair, Committee on Education



Alexa Aviles
Council Member – District 38

⁴ Parent Coalition for Student Privacy, Letter to DOE Chief Privacy Officer Dennis Doyle, October 21, 2024 at: <https://classsizematters.org/wp-content/uploads/2024/10/Serious-concern-with-proposed-Chancellors-regulation-A-820-10.21.24-1.pdf>

The parent emails are here: https://actionnetwork.org/letters/email-to-cpo-pep-members-chancellor-etc-re-privacy-regulations?clear_id=true

⁵ <https://dos.ny.gov/what-you-should-know-about-child-identity-theft>

⁶ See Letter to the NYC Department of Health from NYCLU, Parent Coalition for Student Privacy, and AI for Families, pointing out that when a student visits the Teenspace website to sign up for services, their personally identifiable information is shared with 15 ad trackers and 34 cookies, as well as Facebook, Amazon, Meta, Google, and Microsoft among other companies, in ways that would be prohibited by Education Law § 2-d. The Department of Health argues that they do not have to abide by this law as they are not an education agency. <https://studentprivacymatters.org/wp-content/uploads/2024/10/NYCLU-PCSP-AIF-response-to-DOHMH-regarding-Teenspace-privacy-violations-2024.10.16.pdf>