# Debilidades Críticas en la Propuesta de Reglamento del Canciller A-820 y la Protección de la Privacidad de los Estudiantes por Parte del DOE


Presentación ante el Grupo de trabajo sobre privacidad de datos de las escuelas de la ciudad de Nueva York

Leonie Haimson, CSM/PCSP

Con el apoyo de Shannon Edwards, AI para Familias


Marzo de 2025

# Razón de la creación del Grupo de Trabajo de Privacidad de Datos

- Después de que se publicaron las revisiones propuestas a la regulación A-820 del Canciller el 13 de septiembre de 2024, Parent Coalition for Student Privacy, AI for Families, NYCLU, AQE y otros defensores enviaron comentarios señalando su debilidad e instando a que se fortalecieran.
- Si bien se realizaron algunos cambios, cuando se volvieron a publicar las normas unas semanas después, seguían siendo muy inadecuadas, como hemos visto. Los padres enviaron más de 3000 correos electrónicos al Canciller y a los miembros del PEP, instando a que se hicieran más revisiones.
- El presidente de la UFT, Michael Mulgrew, envió una carta de apoyo al canciller, expresando sus preocupaciones, al igual que la presidenta de Educación de la Ciudad de Nueva York, Rita Joseph, y los CM Shekar Krishnan y Alexa Aviles, señalando los peligros para la privacidad y seguridad de los estudiantes si se adoptaban estas regulaciones.
- En Noviembre nos reunimos con la canciller y ella aceptó crear un grupo de trabajo sobre privacidad de datos para mejorar las normas y otras políticas y prácticas de privacidad del DOE.
- Esperamos que esta colaboración sea productiva y conduzca a una mayor protección de la privacidad de datos para los estudiantes de la ciudad de Nueva York.

# NYS Ed Law §2-d: ley de privacidad estudiantil bastante fuerte aprobada en 2014 como resultado de la controversia de inBloom

- inBloom Inc. se lanzó en febrero de 2013 con más de 100 millones de dólares en fondos Gates, diseñado para recopilar datos personales de millones de estudiantes de escuelas públicas en 9 estados y distritos, y compartirlos con proveedores con fines de lucro para construir sus herramientas de tecnología educativa.

- Muchos padres, educadores y líderes de distrito protestaron y todos los estados y distritos participantes se retiraron de inBloom. El último fue Nueva York, cuando la Legislatura aprobó un proyecto de ley que exigía esto, en Marzo de 2014. En Abril de 2014, inBloom cerró sus puertas.

- Al mismo tiempo, la Legislatura de Nueva York también aprobó la nueva ley de privacidad Ed Law §2-d; después de años de demora, SED finalizó las regulaciones para la ley en Enero de 2020. Cubre todas las escuelas públicas, escuelas charter y ciertas escuelas preescolares y no públicas, descritas aquí.

- En Junio de 2014, se fundó la Coalición de Padres para la Privacidad de los Estudiantes ya que nosotros, junto con otros padres de todo el país, nos dimos cuenta de que las leyes federales sobre privacidad no eran lo suficientemente estrictas. Poco después, se aprobaron más de 100 nuevas leyes estatales sobre privacidad de los estudiantes. Sin embargo, el DOE nunca ha cumplido plenamente con el artículo 2-d de la Ley de Educación y ahora propone revisar las Regulaciones A-820 del Canciller para debilitar sus protecciones de privacidad.

# ¿Cómo protege el artículo 2-d de la Ley de Educación la privacidad de los estudiantes?

- Ley de Educación § 2-d Todo proveedor escolar con acceso a información personal identificable de los estudiantes debe tener un anexo de privacidad que establezca cómo se protegerán esos datos y ese documento debe publicarse en el sitio web del distrito.
- La información de identificación personal debe estar cifrada en todo momento con un alto nivel de seguridad, como lo especifica la versión 1.1 del Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología.
- El acceso de los proveedores a la información de identificación personal (PII) debe minimizarse y eliminarse cuando ya no sea necesario para llevar a cabo los servicios contratados.
- Se debe informar a los padres cómo pueden acceder a los datos de sus hijos que tiene el DOE o el proveedor y cuestionarlos si son inexactos.
- Se debe notificar a los padres dentro de los 60 días posteriores a que el distrito tenga conocimiento de una violación de datos.
- La información de identificación personal (PII) de los estudiantes no se puede vender ni utilizar con fines comerciales o de marketing, incluido el uso para mejorar productos o crear nuevos.
- Los padres pueden presentar quejas al distrito o al estado si los datos de sus hijos se han divulgado de forma indebida.
- Los proveedores pueden ser penalizados económicamente si no cumplen con la ley o se les puede prohibir firmar contratos futuros.

# ¿Qué es la información de identificación personal del estudiante o “PII”?

- El nombre de un estudiante y el nombre de sus padres u otros miembros de la familia;
- Su información de contacto, incluido el teléfono, el correo electrónico, la dirección de su casa o la dirección IP, según su red Wi-Fi o enrutador;
- Identificadores personales, como el número de seguro social, el número de identificación del estudiante o registros biométricos;
- Otros identificadores indirectos, como la fecha de nacimiento, el lugar de nacimiento o el apellido de soltera de la madre;
- Registros educativos y de salud de la escuela, ya sea en forma de documentos impresos, fotos, películas, archivos de audio o video que podrían identificarlos.
- Cualquier otra información, incluida la escuela, la etnia, el grado o la clase, que por sí sola o en combinación podría identificar al estudiante con una certeza razonable.
- Todos estos datos se pueden compartir con proveedores y otros terceros de acuerdo con Ed Law 2d, si están realizando servicios para escuelas o con fines de investigación, siempre que estén bajo el control directo de la escuela.
- Esto generalmente significa un acuerdo o contrato escrito que explica cómo se recopilará la PII y se usará solo para ese propósito específico y se protegerá de una mayor divulgación.

# ¡El Departamento de Educacion ahora propone DEBILITAR en lugar de fortalecer las regulaciones de privacidad del Canciller!

- La reglamentación A-820 del Canciller sobre la privacidad de los estudiantes no se había actualizado desde 2009; sin embargo, las revisiones propuestas pondrían en grave peligro la privacidad de los estudiantes y, en nuestra opinión, NO están alineadas con la ley estatal.
- Ejemplo: el DOE y/o las escuelas individuales podrían compartir una amplia gama de información de identificación personal (PII) casi ilimitada y altamente confidencial sin el consentimiento de los padres y con quien quieran, llamándola Información de directorio y solo un método poco confiable de exclusión voluntaria de los padres para protegerla.
- Los datos *"incluirían, entre otros, lo siguiente: nombre; dirección; número de teléfono; dirección de correo electrónico; fotografías; fecha de nacimiento; nivel de grado; estado de inscripción; fechas de inscripción (pero no asistencia diaria o por período de clase); participación en actividades y deportes oficialmente reconocidos; peso y altura de los miembros de equipos deportivos; títulos, honores y premios recibidos; y escuelas a las que asistió".*
- Sin embargo, esto ignora que NO hay mención en la Ley Ed 2D de la Información de Directorio ni ninguna exención de sus protecciones de privacidad obligatorias, para garantizar que esta PII altamente sensible no caiga en las manos equivocadas para ser abusada o divulgada nuevamente.

# Las regulaciones propuestas también omiten importantes normas de seguridad

- La Ley de Educación 2D exige que las escuelas utilicen el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología, un conjunto de pautas que ayudan a proteger contra las infracciones; no se menciona esto en las regulaciones
- Las revisiones del DOE no mencionan la necesidad de que los proveedores eliminen datos cuando la información ya no es necesaria para llevar a cabo sus servicios.
- Violaciones de datos de Illuminate y Moveit expusieron cientos de miles de exalumnos de la ciudad de Nueva York cuyos datos deberían haber sido eliminados hace años
- En cambio, las regulaciones propuestas dicen: "Proteger la información de identificación personal cuando se almacena o transfiere mediante el uso de cifrado, cortafuegos y protección con contraseña, y garantizar que dichas salvaguardas cumplan con los estándares de la industria y las mejores prácticas".
- Sin embargo, como hemos visto en las reiteradas violaciones de datos de estudiantes, en la ciudad de Nueva York y en todo el país, ¡los estándares actuales de la industria de tecnología educativa NO son las mejores prácticas!

# La definición de DI del DOE de la ciudad es contraria al propio asesoramiento del DOE y la orientación del NYSED

- Estas revisiones ignoran la declaración del DOE en su sitio web de que las ***direcciones de domicilio, los números de teléfono y las fechas de nacimiento son demasiado confidenciales para ser considerados información de directorio.***

- **Como dice el DOE sobre la ciberseguridad:** *"Nunca proporcione información de identificación personal (PII)… incluyendo su fecha de nacimiento completa, número de teléfono… o dirección de domicilio".*

- El Departamento de Estado de Nueva York advierte que el robo de identidad de menores puede ocurrir con solo unos pocos elementos de datos personales, como el nombre y la fecha de nacimiento, lo que podría dañar seriamente sus perspectivas, ya que los delitos como el robo de identidad pueden pasar desapercibidos durante años:

- *"El robo de identidad infantil ocurre cuando alguien usa la información personal de un menor, como el nombre y la fecha de nacimiento… El daño causado por el robo de identidad infantil puede variar desde una sola factura fraudulenta en cobros hasta una hipoteca ejecutada."*

- La divulgación de estos datos también podría conducir a la explotación comercial, la victimización sexual, el acoso cibernético, el secuestro y/o los esfuerzos de deportación del gobierno..

# Los registros médicos y de salud no están suficientemente protegidos

- Los registros médicos y de salud de los estudiantes sensibles en las escuelas NO estarían protegidos por la Ley de Educación 2D si los hiciera el personal del Departamento de Salud de la Ciudad de Nueva York u otros funcionarios, en las clínicas de salud y salud mental de las escuelas.

- La Ley de Educación 2D no exime los registros que mantienen las escuelas, ya sea que los haga el personal de la escuela, los empleados de otras agencias de la ciudad o las organizaciones comunitarias que brindan servicios escolares comunitarios.

- La guía federal dice: "*Los registros de salud que se relacionan directamente con los estudiantes y que son mantenidos por un proveedor de atención médica, como un contratista externo... calificarían como registros educativos sujetos a la FERPA independientemente de si el proveedor de atención médica es empleado de la escuela.”*

- Ya hemos visto cómo se puede abusar de los datos de los estudiantes cuando NO están protegidos por la Ley de Educación 2D, como en el caso del Departamento de Salud de la Ciudad de Nueva York, que ha permitido que Talkspace explote datos de salud mental sensibles con fines comerciales y los comparta con compañías de redes sociales.

# ¿Qué pasa con la necesidad de que las escuelas contraten empresas para producir anuarios, etc.?

- Las preguntas frecuentes del Departamento de Educación de Nueva York explican cómo las escuelas pueden seguir permitiendo que las empresas de anuarios, los fotógrafos y otros proveedores de servicios recopilen y utilicen datos personales de los estudiantes con el fin de producir sus productos.

- Sin embargo, estas escuelas deben asegurarse de tener contratos escritos con sus proveedores que cumplan plenamente con la Ley de Educación § 2-d, incluida la limitación del uso de la información personal identificable de los estudiantes para llevar a cabo estos servicios, prohibir futuras divulgaciones y eliminar los datos cuando ya no sean necesarios.

- Escriben: “Si bien el contrato con el proveedor debe cumplir con los requisitos para contratistas externos que se encuentran en la Ley de Educación § 2-d y la Parte 121 de las regulaciones del Comisionado, el proveedor no tiene prohibido realizar actividades de conformidad con el contrato para proporcionar el servicio contratado. Dichas actividades pueden incluir notificar a los padres sobre las sesiones de fotografía de las clases y las ventas de anuarios, ya que esto sería parte del servicio que está brindando a la agencia educativa”.

- Es especialmente importante que estos acuerdos requieran muros de pago y eliminación, ya que delincuentes pueden extraer imágenes de alta calidad de la web mediante inteligencia artificial para crear pornografía falsa o acusaciones falsas de secuestro, poniendo a los niños en riesgo de explotación y daño.

# El DOE también comparte información de estudiantes/padres con las escuelas Charter para ayudarlas a reclutar estudiantes.

- Durante años, el DOE afirmó que esto era legal, ya que solo proporciona indirectamente las direcciones de las familias, etc., a través de su servicio de correo
- Sin embargo, muchos padres ahora informan que también reciben una avalancha de llamadas telefónicas de las escuelas autónomas
- Si bien el DOE afirma que los padres pueden optar por no recibir estos correos, pero incluso después de que los padres completen el formulario de exclusión, muchos dicen que todavía reciben una avalancha de correos y llamadas telefónicas, lo que demuestra lo falible que es el proceso de exclusión
- NYC es el único distrito del país que proporciona esta información personal de los estudiantes de manera voluntaria a las escuelas autónomas

NYC Department of Education

## 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.

Close

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 *

# A pesar de los mandatos de Ed Law 2-d, los procesos laxos de seguridad y contratación del DOE ya provocaron filtración de datos

- ***A partir de diciembre de 2024, al menos 523 empresas de tecnología educativa, 55 proveedores de servicios relacionados y 50 grupos de investigación tenían anexos de privacidad en el sitio del DOE, lo que significa que tienen acceso a la información personal identificable de los estudiantes de la ciudad de Nueva York.***

- Sin embargo, muchas empresas con acceso a la información personal identificable de los estudiantes no tienen acuerdos de privacidad publicados en el sitio web del DOE, incluidas algunas que sufrieron filtracion de datos.

- Además, muchos de los acuerdos de privacidad que SÍ están publicados NO se ajustan completamente a la ley.

- Ejemplo: en enero de 2022, la violación de Illuminate expuso los datos personales de más de un millón de estudiantes actuales y anteriores de la ciudad de Nueva York, incluidas las fechas de nacimiento, la etnia, los registros académicos, la educación especial y/o el estado de almuerzo gratuito, incluidos miles de exalumnos.

- Cuando el acuerdo de privacidad del DOE con Illuminate se publicó posteriormente, insinuó que la información personal identificable NO siempre estaba cifrada. Aunque se ofrecieron auditorías de seguridad, no hay indicios de que el DOE las haya solicitado alguna vez

- En mayo de 2023, la filtración de MoveIt divulgó información de identificación personal de 45 000 estudiantes, además del personal del DOE y los proveedores de servicios relacionados, sin que se publicara ningún anexo ni contrato de privacidad.

# El contralor estatal determinó que el DOE no había notificado adecuadamente las infracciones


- El contralor estatal informó que el 80% de los informes de incidentes de ciberseguridad del DOE carecían de detalles suficientes para determinar si los estudiantes y los maestros fueron informados dentro del plazo de 60 días requerido por la ley.
- En más de la mitad de los incidentes, el DOE de la ciudad de Nueva York superó el plazo legal para notificar el problema al NYSED.
- Y, sin embargo, el DOE de la ciudad de Nueva York sigue ampliando el uso de la tecnología educativa y el aprendizaje en línea, incluidos programas de inteligencia artificial riesgosos, multiplicando el riesgo de violaciones de datos y mal uso de los datos de los estudiantes, sin las medidas de protección necesarias y ahora proponiendo debilitar las normas de privacidad del Canciller A-820.

# Violación de datos de PowerSchool en Diciembre de 2024

- El 9 de Enero de 2025, PowerSchool anunció que, a fines de Diciembre, el sistema de información de estudiantes de PowerSchool había sido hackeado, lo que expuso la información personal identificable de los estudiantes de muchos distritos y escuelas de todo el país, y comenzó a informarles sobre la violación.

- Entre los datos publicados, según la escuela y el distrito, se encontraban los nombres de los estudiantes, la información de contacto, la fecha de nacimiento, las calificaciones, los puntajes de las pruebas, el estado de educación especial, los detalles de salud mental, las notas disciplinarias, las órdenes de restricción de los padres y más, así como la información personal identificable de los maestros en algunos distritos.

- Inicialmente, el DOE les dijo a los periodistas que ninguna escuela de la ciudad de Nueva York se vio afectada.

- El 3 de Febrero de 2025, NYSED me alertó de que el DOE les había dicho que al menos cuatro escuelas de la ciudad de Nueva York que inscriben a unos 3000 estudiantes probablemente se vieron afectadas; sin embargo, el DOE se negó a confirmarlo cuando un periodista le preguntó.

- Al 26 de Febrero de 2025, el DOE todavía no había dicho nada públicamente ni publicado ninguna alerta en su sitio web, a pesar de la orientación del NYSED de que esto debería hacerse "para captar la mayor audiencia posible", especialmente porque los ex alumnos también pueden haberse visto afectados y la empresa ofrecía un seguro gratuito contra robo de identidad y monitoreo de crédito.

- El sitio web del DOE finalmente se actualizó el 2 de Marzo, más de 2 meses después de que sucedió la filtración, pero se negó a revelar qué escuelas o qué datos se vieron afectados, aunque se les dijo a los padres de LICHS que los ex alumnos también podrían haber tenido su información violada

# El acuerdo de privacidad del DOE con PowerSchool es defectuoso y NO se ajusta a la ley.

- PowerSchool enfrenta ahora numerosas demandas estatales por prácticas de privacidad laxas, incluida la falta de uso de autenticación doble, un procedimiento estándar para proteger la seguridad de la información de identificación personal.
- Pero, como señalamos hace meses, el acuerdo de privacidad de PowerSchool con el DOE dice que la empresa "revisará las políticas y prácticas de seguridad y privacidad de datos para garantizar que cumplan con todas las leyes federales, estatales y locales aplicables y los términos de este DSPP [Plan de privacidad y seguridad de datos]…
- *… En caso de que las políticas y prácticas del procesador no cumplan, el procesador implementará esfuerzos comercialmente razonables para garantizar dicho cumplimiento."*
- En otras palabras, PowerSchool **solo cumplirá con las leyes federales y estatales de privacidad cuando no afecte indebidamente sus resultados.**

# AÚN así, el DOE autoriza a las escuelas a utilizar 17 productos PowerSchool que consumen muchos datos, incluido Naviance, que comercializa datos de estudiantes


- Naviance, un programa de planificación universitaria y profesional, se utiliza en muchas escuelas secundarias de la ciudad de Nueva York, que recopila una gran cantidad de información personal identificable de los estudiantes y envía anuncios dirigidos a los estudiantes, disfrazados de recomendaciones objetivas, en violación de la ley estatal. Se ha demostrado que la empresa permite a las universidades discriminar al dirigir los anuncios solo a los estudiantes blancos.

- Otros programas de PowerSchool que el DOE permite que utilicen las escuelas de la ciudad de Nueva York y que recopilan información personal identificable de los estudiantes: *Enrollment, Enrollment Express, Performance Matters Advanced Reporting; Performance Matters Assessment;* y *PowerSchool SIS*

- Datos de estudiantes y maestros: *Unified Talent Employee Records; Unified Classroom Schoology Learning; Unified Classroom Curriculum and Instruction*

- Datos de educación especial, SEL y comportamiento: *Unified Classroom Special Programs; Unified Classroom Behavior Support,* ¡y seis más!

- **No se debe confiar en ninguno de estos programas dadas las prácticas de privacidad descuidadas de PowerSchool y la debilidad inherente del contrato del DOE.**

# College Board, un conocido violador de la ley estatal de privacidad de los estudiantes

- Durante años, College Board ganó más de $100 millones anuales vendiendo datos personales de estudiantes recopilados durante las pruebas en la escuela y cuando se registran para obtener cuentas.
- Esto incluye nombres de estudiantes, direcciones, raza/etnia, calificaciones, ingresos y rangos de puntaje de exámenes, a pesar de que esta venta ha violado la ley de privacidad estudiantil en Nueva York desde 2014.
- Protestamos por esta práctica ante el DOE y no hicieron nada para detenerla.
- Finalmente, en febrero de 2024, el Fiscal General de Nueva York negoció un acuerdo de consentimiento con College Board y acordaron detener esta práctica y pagar una multa de $750,000.
- Pero no tenemos idea de cómo se aplicará o monitoreará esto, especialmente porque **el DOE no tenía un contrato vigente con College Board desde junio de 2023**, ¡incluso cuando cientos de miles de estudiantes de escuelas secundarias de Nueva York tomaron exámenes AP, PSAT y SAT el año pasado en la escuela y el DOE les pagó millones por esas pruebas!

# College Board: otro acuerdo de privacidad débil del DOE

- El acuerdo de privacidad de CB publicado en el sitio web del DOE dice que la empresa y sus subcontratistas NO encriptará los datos de los estudiantes “cuando los datos no puedan encriptarse razonablemente”
- También dice que eliminará los datos solo “cuando todas las escuelas y/o oficinas del DOE de Nueva York dejen de usar los productos/servicios de College Board.”
- Para el SAT/PSAT, el PBOR no contiene una fecha ni una hora específicas en las que se eliminarán los datos; ambas son contrarias a la ley.
- Recientemente, se presentó un proyecto de ley para crear un vacío legal en la Ley de Educación 2D para permitir que College Board continúe monetizando los datos de los estudiantes
- A9967/ S9597 permitiría a CB enviar anuncios dirigidos a los teléfonos de los estudiantes, pagados por las universidades y otras empresas, en función de sus datos, incluidas sus calificaciones, puntajes de exámenes, raza y etnia

# ¿Cuál es el daño de las violaciones de datos o la divulgación de información personal identificable de los estudiantes sin restricciones?

- La información personal identificable de los estudiantes es muy valiosa para el robo de identidad, ya que la mayoría de los menores no tienen calificaciones crediticias
- El control excesivo del uso de Internet de los estudiantes por parte de las escuelas puede ser devastador para su sentido de libertad individual
- Las escuelas también pueden utilizar sus datos para elaborar perfiles raciales, aplicar la ley y realizar otras acciones discriminatorias
- Las empresas de tecnología publicitaria y redes sociales pueden utilizar la información personal identificable de los estudiantes para fines de marketing, bombardeándolos con anuncios e incluso socavando su salud mental, como se señaló en demandas recientes de la ciudad de Nueva York y del estado contra estas empresas
- La información negativa sobre un estudiante puede afectar sus oportunidades futuras, incluidos empleos, admisión a la universidad, seguro médico, etc.
- Los datos de los estudiantes también pueden utilizarse para amenazar su seguridad, lo que conduce al acoso cibernético, el acoso sexual, el abuso, el secuestro o la deportación

# El DOE también comparte información de estudiantes y padres con las escuelas Charter para ayudarlas a reclutar estudiantes.

- Durante años, el DOE afirmó que esto era legal, ya que solo proporciona indirectamente las direcciones de las familias, etc., a través de su servicio de correo
- Sin embargo, muchos padres ahora informan que también reciben una avalancha de llamadas telefónicas de las escuelas Charter
- Si bien el DOE afirma que los padres pueden optar por no recibir estos correos, pero incluso después de que los padres completen el formulario de exclusión, muchos dicen que todavía reciben una avalancha de correos y llamadas telefónicas, lo que demuestra lo falible que es el proceso de exclusión
- NYC es el único distrito del país que proporciona esta información personal de los estudiantes de manera voluntaria a las escuelas Charter

NYC Department of Education

## 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

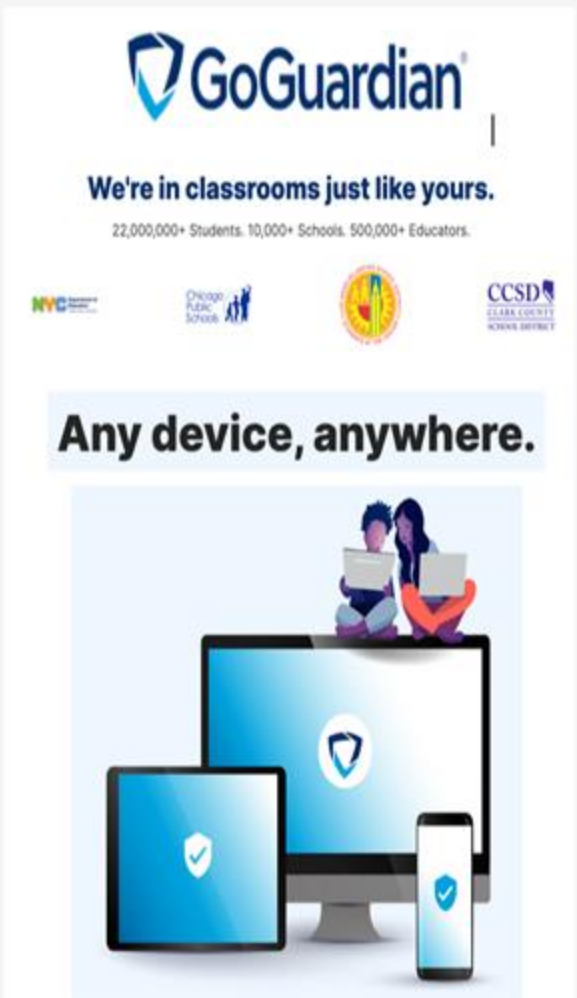
If you wish to receive these mailings, you do not need to do anything. If you do not wish to receive charter school informational mail, please fill out and submit the survey **no later than October 31.** If you miss this deadline, you can submit the survey by **January 15** to stop receiving the mailings 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.

Close

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 *

# Algunas escuelas de Nueva York también vigilan a los estudiantes sin alertar a los padres




- En Octubre de 2021, Bloomberg News informó que el Departamento de Educación de la Ciudad de Nueva York firmó un contrato con GoGuardian, que vende software espía/de vigilancia instalado en las computadoras que utilizan los estudiantes y que podría espiar sus hogares y a sus familiares sin su conocimiento si no se configura correctamente.

- Cuando un miembro del PEP pidió ver este contrato en Noviembre de 2021, el DOE dijo que no había ninguno, pero que "podían poner este producto a disposición de todas las escuelas de manera centralizada a través de la licencia Enterprise G-Suite/Google Workspace sin costo para la escuela ni para las familias".

- Más recientemente, el DOE publicó en línea un acuerdo de privacidad de GoGuardian, para un contrato que, según dicen, comenzó en Agosto de 2021, pero carece de suficientes detalles y dice que caducó en Agosto de 2024.

- Según GoGuardian, la mejor práctica es informar a los padres de antemano de que este programa se está utilizando e instalando en las computadoras de sus hijos, y permitir que los padres opten por no participar, pero no sabemos si esto se ha hecho en las escuelas de la ciudad de Nueva York.

# La expansión de la Inteligencia Artificial (AI) podría socavar aún más la privacidad de los estudiantes


- El DOE alienta a los directores y maestros a expandir el uso de AI sin orientación, aunque la mayoría de los programas de AI generativa recopilan datos personales para mejorar sus productos, como lo señala la queja de la FTC del Centro de Inteligencia Artificial y Política Digital.

- Open AI admite que *"**Chat GPT-4 tiene el potencial de usarse… para identificar a individuos privados cuando se amplía con datos externos**"* y que su uso podría *"**reforzar y reproducir sesgos y visiones del mundo específicos, incluidas asociaciones estereotipadas y degradantes dañinas para ciertos grupos marginados**".*

- Su política oficial dice que ningún niño menor de 13 años debe usar Chat GPT, y ningún estudiante de entre 13 y 17 años sin el consentimiento de los padres. Otros programas de AI tienen restricciones similares vinculadas a la edad que muchas familias y escuelas ignoran.

- Sin embargo, el DOE NO ha publicado ninguna guía ni barreras para garantizar que los datos de los estudiantes no se moneticen ni se abusen a través del uso de AI en las aulas y las escuelas. Una vez que se comparten con la AI, es imposible verificar si no se extrajeron de manera indebida.

- HMH Writeable, autorizado para usarse en las escuelas de la ciudad de Nueva York, dice que utiliza datos de los estudiantes para ***"mejorar el producto"*** en su Política de privacidad, y su acuerdo de privacidad con el DOE no lo prohíbe.