# CHIEF PRIVACY OFFICER'S 2024 ANNUAL REPORT ON DATA PRIVACY AND SECURITY

Pursuant to Education Law § 2-d, the New York State Education Department's (NYSED) Chief Privacy Officer is required to issue an annual report on:

(1) Data privacy and security activities and progress,
(2) The number and disposition of reported breaches, if any, and
(3) A summary of any complaints of possible breaches of student data or teacher or principal annual professional performance review (APPR) data.

This report addresses the reporting period of January 1 to December 31, 2024.

## I. Opening and Summary of Data Privacy and Security Activities and Progress

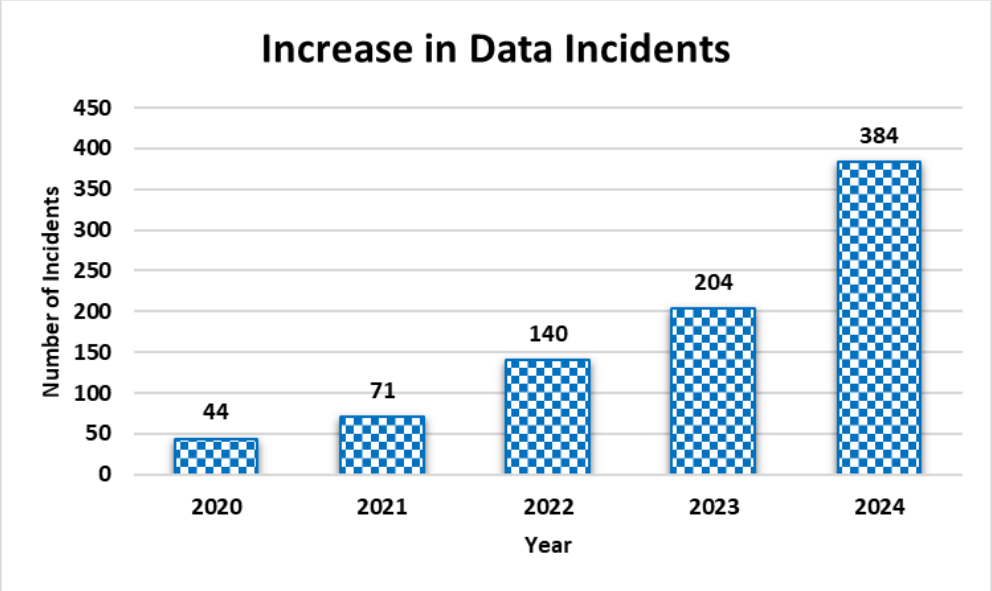
As I prepare my fourth Annual Report, I have found myself reflecting on the role transparency plays in Education Law Section 2-d. Indeed, the desire for transparency is what created the requirement that my office issue an Annual Report. Transparency is at the heart of both Education Law Section 2-d and the Family Educational Rights Privacy Act (FERPA), the two primary education privacy laws we comply with in New York[1]. When I do presentations or trainings on these two laws, I often spend a few minutes explaining the advocacy that created these laws. For example, when it became public that parents did not have access to their children's education records, New York Senator James Buckley led the charge to create FERPA, which was signed into law in 1974. Forty years later, in 2014, New York's legislature responded to advocates opposed to the significant data sharing requirements in New York's Race to The Top application and subsequent award. Although the advocates lost their litigation against NYSED, the legislature made sure that they were heard when it created Education Law Sections 2-c and 2-d.

At a recent conference, several attendees thanked me for the Privacy Office's willingness to share information with the field through our website. Not only is the information a matter of transparency for parents and taxpayers, but it also assists researchers and advocates

[1] This is not to minimize the importance of the Children's Online Privacy Protection Act (COPPA), the Protection of Pupil Rights Amendment Act (PPRA), the Individuals with Disabilities Education Act (IDEA), New York's Personal Privacy Protection Law (PPPL) and other laws that protect student privacy in New York's educational agencies.

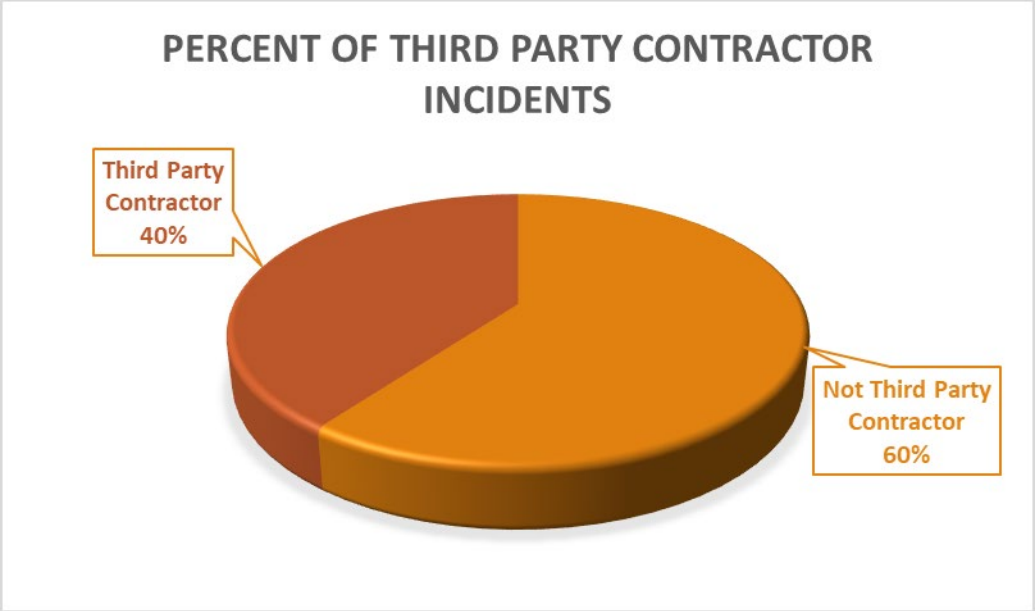
working on privacy issues throughout the world. Particular attention was paid to the Privacy Office's complaint determinations (which are summarized annually in this report), our enforcement case resolutions, and to the Annual Report. The Annual Report is an opportunity for the Privacy Office to summarize the incidents we've seen over the past year and provide specific examples so that anyone reading this report gains insight into the current state of data privacy and security in New York's educational agencies[2].

Similar to the last three Annual Reports, 2024 saw a continued increase in reported data incidents and breaches. Reports to the Privacy Office have increased annually and grown from 44 in 2020 to 384 in 2024. As in the past, most incidents reported to the Privacy Office arose from human error, typically the inadvertent transmission of information to an unrelated party via email or attachment. Section II of this report includes examples of the types of human error breaches reported in 2024.




Additionally, approximately 40 percent of this year's incidents (152 incidents) involved third party contractors or vendors. This is a higher percentage than in 2023 (30 percent), in large part due to two third party contractor incidents that affected 135 educational agencies. Enforcement was taken against these third party contractors who resolved their cases through an order on consent. Although one of these third party contractor cases was caused by a phishing incident, the good news is that in 2024 only ten educational agencies reported falling prey to phishing compared to 23 phishing incidents in 2023. Phishing exercises remain a best practice for educational agencies to ensure that their staff are properly prepared to handle phishing emails.

[2] Education Law § 2-d defines educational agency as a school district, board of cooperative educational services (BOCES), school or NYSED. Schools are defined to include charter schools.




In addition to the increase in data incident reports, the Privacy Office received 30 privacy complaints that resulted in eight written determinations. Of the 22 complaints that did not result in a written determination, 17 parents received a letter explaining why the Privacy Office was unable to render a determination or that the matter was resolved. The Privacy Office had no jurisdiction over five complaints because they pertained to a private school or a college or university. Section IV of this report contains a more detailed description of the complaint determinations.

For 2025, the Privacy Office has multiple goals, including:

1) Respond to the PowerSchool data breach, perhaps the Country's largest data breach to affect students. Ascertaining what New York educational agencies were affected; whose data within the educational agency was breached and the appropriate enforcement action to be taken will be a top priority for 2025.
2) Continuing our important work with the Regional Information Centers (RICs) to offer all of New York's educational agencies student data privacy consortium memberships and access to the National Data Privacy Agreement. The State's membership in Access for Learning (A4I) and the RICs' membership in The Educational Cooperative (TEC) continue to assist educational agencies with drafting, negotiating, and managing standardized Data Protection Agreements (DPAs) for third party contractors and vendors.
3) Review Part 121 of the Commissioner's regulations with the goal of offering proposed amendments. At a minimum, the regulations need to be amended to change the reference to the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 to Version 2. This presents an opportunity to consider whether other aspects of Part 121 should be amended also.
4) Issue additional guidance on Directory Information.

5) Continued engagement with internal and external stakeholders, particularly superintendents, school board members and charter schools.

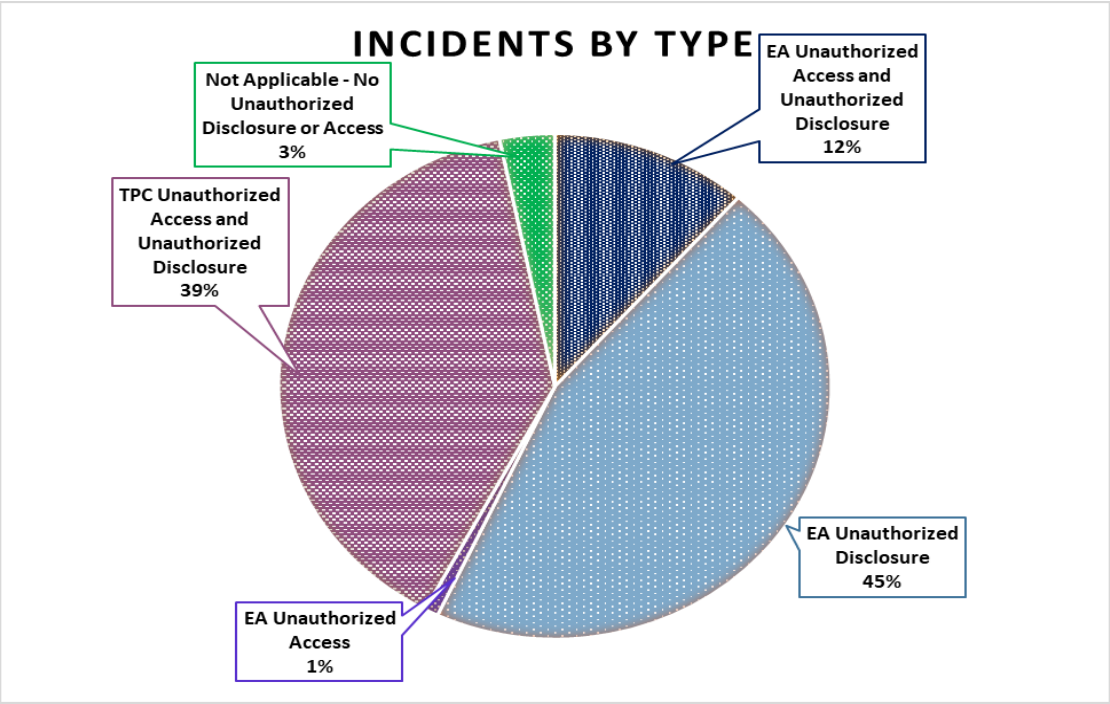
Sections II and III of this report analyze and describe reported breaches. This summary includes the disposition of data incident report filings. Section IV of this report summarizes complaints concerning possible breaches of student or certain teacher/principal data during 2024 and the Privacy Office's disposition thereof. Section V discusses the Privacy Office's 2024 monitoring of educational agencies' web sites for compliance with FERPA, Education Law § 2-d and Part 121 of the Commissioner's regulations. Section VI discusses enforcement actions taken by the Chief Privacy Officer.

The Privacy Office looks forward to continued collaboration with our external stakeholders: school districts, charter schools, State-approved special education schools, Boards of Cooperative Educational Services (BOCES) and Regional Information Centers (RICs), parents and advocates as well as our internal stakeholders at NYSED, as we continue to provide guidance about the legal and regulatory requirements and importance of data privacy and security.

Louise DeCandia
Chief Privacy Officer

## II. Reported Breaches 2024

In 2024, the Privacy Office received 384 data incident reports from 100 different educational agencies, an 88 percent increase from the 204 incidents reported in 2023. Of these 384 incidents, 152 were caused by third party contractors. Approximately 200 of the reported data incidents were due to human error within educational agencies, 10 were due to phishing attacks, 3 to an external breach or hacking, none to ransomware and malware attacks, 14 to insider wrongdoing, and 7 to other incidents such as theft of a device. The 2024 data incidents by type can be viewed in the chart below.




## Human Error and Unauthorized Disclosures

In preparation for this report, the Privacy Office reviewed the 2024 data incident reports in detail. As in previous years, human error accounted for a majority of the 2024 incident reports. At least 84 reports involved personally identifiable information (PII) being sent to the wrong individual. Examples include:

- A student's Committee on Special Education (CSE) meeting information and absenteeism information was mistakenly sent to 72 parents.
- A student's discipline referral was emailed to an assistant principal in a neighboring school district.

- A mail merge which was incorrect because one student recently left the school, caused 2,340 families to be sent other children's information regarding vaccine status.
- A teacher sent a link to Google Homework calendar with student information at the bottom identifying seven students in jeopardy of failing.
- An email with a student's immunization record was accidentally sent to the entire school.
- A school counselor accidentally attached a student's PSAT score to an email that was sent to 30 students.
- A guidance counselor took part in a virtual CSE meeting in an open space with no headset, allowing others to hear the meeting.
- A school social worker reviewed students' grades with them while they were waiting on a line to meet with their guidance counselor.

Several teachers and staff caused breaches by improperly using their educational agency's tools such as Parent Square, Class Dojo, Jupiter Messaging, GAMMA, Remind and YouTube.

*Data incidents involving paper documents are still occurring:*

- One school used paper student education records to mulch their plants.
- One teacher left a binder with nine students' Individualized Education Programs (IEPs) on a classroom table at the end of a school day. The teacher was out sick the following day and when they returned to the classroom, the binder was gone.
- Student health records were put in boxes to be transported from the middle school to the high school as part of the process for rising ninth grade students. The boxes were discarded by the educational agency's custodians.
- Students' report cards were printed back-to-back causing approximately 210 students to receive other students' report cards.

*Social Media and Website Postings*:

- A student created an account on TikTok using students' school pictures and asked for comments on whether matched-up students should be in a relationship. The student accessed the picture proofs by figuring out a weak password system.
- While trying to post the honor roll list to Facebook, a school staff member inadvertently posted the entire SchoolTool report with each students' identification number and quarterly grades.
- A principal accidentally posted a picture of a student-discipline related incident (a photograph of cannabis gummies with two students' names) while posting pictures of a basketball game on the educational agency's website.
- A Facebook post created by an educational agency's staff member included a picture of a student using their Chromebook, visibly showing the student's username and password in the picture.

*2024 had many instances of students obtaining improper access to school accounts*:

- One student brought a spreadsheet to school showing files he was able to access in one of the school's drives. The files were mistakenly left after the school transitioned to Google.
- A staff member's child used her parent's SchoolTool account to access three student's accounts.
- Student A asked B for help logging in to their account. Student B took student A's password and viewed their grades.
- After discovering changed grades, one educational agency realized that a teacher's password was compromised by a student.
- One educational agency posted a QR code throughout the school providing access to 167 students' information.
- In one educational agency a teaching assistant shared her SchoolTool log in information with her daughter resulting in student's gaining access for a period of two years. Criminal prosecutions ensued.
- A substitute teacher left out a class roster which was picked up by a student who then sent inappropriate messages to the other students.
- Students obtained administrative access to the Educational Agency's Google and SchoolTool accounts by obtaining the log-in credential of a former staff member.
- One student randomly tried usernames until they were able to log into other students' accounts.

*2024 also had several instances where data protection officers (DPOs) stopped their educational agency from proceeding to use education technology tools that did not have a data protection/privacy agreement (DPA) in place*:

- When investigating an overloaded WIFI connection a DPO realized that an assessment tool that did not have a DPA was being used. The DPO stopped the use of the assessment immediately.
- In one school, staff used a non-approved scheduling app to schedule CSE meetings, until the DPO discovered this was occurring and put an end to it.
- In another school, a teacher gave a vendor unauthorized access to a platform to help resolve an issue until the DPO intervened.

*Particularly problematic incidents*:

- A staff member took a screenshot of an email regarding an incoming student who identifies as non-binary and shared the information outside of the educational agency.
- In one educational agency, two staff members downloaded email addresses of 238 parents from the student information system to send out information regarding a tutoring service they created.
- A principal mistakenly downloaded and attached hundreds of his emails as part of the educational agency's civic readiness filing to NYSED. The emails contained extensive PII and notes on teacher classroom reviews and were all vetted through Chat GPT.
- A teacher who resigned downloaded and deleted student files affecting 1,550 students.

## Third Party Contractors

Approximately 40 percent of the data incident reports filed in 2024 (152 incidents) involved third party contractors or vendors. Of the 152, 135 data incident reports involved two third party contractor breaches that occurred in 2023; Raptor Technologies and New York Therapy. Enforcement actions were taken against the third party contractors. Additional information on these breaches is provided below.

- The Raptor Technologies incident involved a vulnerability discovered by a security researcher who disclosed it on December 20, 2023. The vulnerability involved cloud-hosted storage containers serving specific features of Raptor Technologies Visitor Management and Emergency Management software. This vulnerability could have allowed the enumeration of files in certain Azure storage containers and potentially rendered such files unsecured and publicly accessible. According to Raptor Technologies there was no evidence that data was taken or accessed by any unauthorized party. 112 educational agencies were affected by this vulnerability.
- An employee of New York Therapy Placement Services, Inc. (NYTPS) fell victim to a phishing email on November 28, 2023. The email appeared to originate from a client school district that, according to NYTPS "typically sends secure e-mails." The compromised employee entered their username and password in response to prompts provided in the email and the employee's email account was subsequently used to send emails. NYTPS provided notice of the breach to 125 educational agencies.

## Phishing

For 2024, the Privacy Office received ten data incident reports pertaining to phishing attacks. This is a 59% decrease from 2023 when the Privacy Office received 23 data incident reports pertaining to phishing.

- As occurred in 2023, several schools received a phishing attack sent to student and employees with the subject line "looking for work."
- Several schools reported receipt of a phishing email using NYSED's logo and identification.
- One phishing attack was targeted to a teacher's payroll account.
- In one educational agency a teacher responded to a phishing email which then created a form sent to 993 students. Eight students filled out the form which was entitled "summer employment".

## Cyberattacks

Although there were a few reported incidents of hacking in 2024, several by students, New York's educational agencies reported no cyberattacks to the Privacy Office during 2024. To confirm this information, the Privacy Office compared its data with data collected by the New York State Division of Homeland Security and Emergency Services (DHSES). DHSES reported that they received reports of two login brute force attacks, three malware

(not ransomware attacks), one malware attack and one ransomware attack from New York's educational agencies during 2024.

## III. Disposition of Data Incident Report Filings

Education Law § 2-d and Section 121.10 of the regulations of the Commissioner of Education require educational agencies to report *every* discovery, or third party contractor notification, of a breach or unauthorized disclosure of student, teacher, or principal data to the Chief Privacy Officer within 10 calendar days of discovery. When a data incident report is filed with the Privacy Office, there may be follow-up discussions with the educational agency to answer additional questions and, more importantly, to determine if PII was released and whether the proper procedures were implemented when a breach has occurred.

Collecting this data allows the Privacy Office to share information about system compromises and breaches within the education field to all of New York's educational agencies. This information can help identify where technical assistance may be necessary and assist educational agencies in improving data privacy and security practices.

## IV. Summary of Privacy Complaints 2024

Section 121.4 of the regulations of the Commissioner of Education and NYSED's § 2-d Bill of Rights for Data Privacy and Security authorize parents, eligible students, teachers, principals, and other staff of an educational agency to file complaints about possible breaches and unauthorized releases of PII. When a complaint is filed with NYSED's Privacy Office, the educational agency is often asked to provide a detailed investigation report. The Privacy Office strives to render timely decisions that assist educational agencies and complainants in understanding the laws, regulations, and requirements pertaining to student, teacher, and principal data privacy and security. Additional investigation may be undertaken directly by the Privacy Office.

In 2024 the Privacy Office received 30 complaints that resulted in 8 written determinations. The Privacy Office did not have jurisdiction over 4 of the 30 complaints. Of the remaining 18 complaints, 17 parents and superintendents received a letter explaining why the Privacy Office did not render a determination, and one parent of a child attending a private school received a phone call and follow-up email. The determinations that were rendered in 2024 are summarized below and are available on the Privacy Office's webpage.

1. Croton Harmon Union Free School District (issued 9/10/24):

   An eligible student complained that the school district inappropriately disclosed his PII when it posted a photograph of him as a graduating student on the district's Instagram and X (Twitter) pages. The eligible student asserted that his father opted out of the district's directory information policy. The school district stated that it had no record of the student's father having filed an opt-out form, and that the picture was voluntarily submitted by the student's mother. The Privacy Office determined that the photograph

at issue was not an education record and therefore no violation was found under FERPA or Education Law § 2-d. The Privacy Office further held that a directory information opt-out form would not apply to the photograph because it was not an education record.

2. Croton Harmon Union Free School District (issued 9/12/24):

   A parent complained that the school district posted pictures of his children on Facebook, Instagram, and X (Twitter) without the parent's consent. The parent admitted that he did not file an opt-out form or withhold consent for the children to appear in district media. The Privacy Office did not find an unauthorized disclosure or release of student PII. However, the Privacy Office encouraged the school to solicit parental input as it prepared its new "Use of Social Media in Instruction and Official Communications" policy.

3. Dryden Central School District (issued 6/26/24):

   Parents asserted that the school district improperly disclosed their children's PII when they determined that requested copies of their education records were missing. The parents had submitted a FERPA request for all their students' education records. After several failed delivery attempts by the school district, it brought the records directly to the parents' home and left them in a sealed box next to the mailbox with their names and address. The parents complained that the box went missing. The Privacy Office found no evidence that the students' education records were improperly disclosed or accessed in violation of FERPA or Education Law § 2-d.

4. Elmira Central School District (issued 2/27/24):

   A parent asserted that the school district violated FERPA and Education Law § 2-d on two occasions. The first incident occurred when the parent requested a copy of her child's test scores and received test scores and other reports of all the students in the child's class. The second incident occurred when the school district shared her child's education record with unauthorized individuals. The school district admitted responsibility regarding the first incident and took appropriate action. Regarding the second incident, the school district claimed the student's record was only shared with school officials who had a legitimate educational interest in the student's records. The Privacy Office determined a breach occurred regarding the first incident. While it could not be determined without additional information that a breach occurred regarding the second incident, the school district was reminded that PII must be shared as minimally as possible.

5. Elmira Central School District (issued 7/19/24):

   Complainant from the previous complaint asserted that the school district inappropriately disclosed other students' PII to her when her child's service provider attached speech language evaluations of two other students to her child's weekly report. The school district did not dispute that the incident occurred and asserted that it handled the issue. The Privacy Office directed the school district to submit a data incident report to the

Privacy Office within five days of the determination, as well as a plan outlining the steps it will take to ensure incidents such as these will not recur.

6. Guilderland Central School District (issued 11/19/24):

   A parent complained that the school district improperly disclosed student PII during an open house when it encouraged students to access their Chromebooks and share a "leaderboard" with the parents in connection with a product used for math. The leaderboard portrayed students' names, scores, and ranks. In the school district's response, it asserted that the leaderboard did not indicate a student's grade, nor did it maintain student information. The Privacy Office found that no breach occurred in violation of FERPA or Education Law § 2-d as the information shared on the leaderboard was not an education record.

7. Katonah-Lewisboro Union Free School District (issued 5/29/24):

   A parent filed two complaints that were consolidated for determination. The first complaint asserted that a school district employee who provided services to her child retained some of the student's education record after leaving her employment. The second complaint asserted that the school district improperly disclosed the student's PII when it authorized its consultant to perform an assessment on the student without the parent's consent. Under the circumstances, the Privacy Office could not find an unauthorized disclosure of PII but advised the parent to reach out to NYSED's Office of Special Education for guidance and assistance regarding the student's IEP.

8. Success Academy Cobble Hill Elementary School (issued 4/30/24):

   A parent asserted that the charter school improperly disclosed her child's PII when it posted the child's name and test scores on a bulletin board in the school hallway. The charter school stated that the parent had received a form regarding the display and did not try to revoke her consent. While the parent admitted to receiving such form, she argued that she did not understand the form to mean student's test scores would be publicly displayed. The Privacy Office agreed with the parent, holding that the form would not be reasonably understood to mean that a student's test scores or grades would be displayed in a manner visible to everyone walking in the hallway. The Privacy Office directed the charter school to submit a revised consent form that must: (1) list the specific records being shared; (2) allow parents, guardians, and eligible students to consent to share some data but not require them to share all data; (3) explain the purpose for sharing the data; (4) explain to whom the disclosure would be made; and (5) provide instructions in the form regarding the right to request a withdrawal of consent in the future.

## V. Monitoring of Educational Agencies' Web Sites

During 2024 the Privacy Office monitored 11 educational agencies in addition to the 120 monitored in 2023. Educational agencies were monitored for the following:

- FERPA Annual Notification to Parents,
- Directory Information Policy,
- Education Law Section 2-d and 121.3(a): Parents' Bill of Rights (PBOR),
- Education Law Section 2-d and 121.4: Information on how parents can file a complaint,
- Education Law Section 2-d and 121.3(d): supplemental information to the PBOR for any contract or other written agreement with a third party contractor that will receive personally identifiable information, and
- Education Law Section 2-d and 121.5(b): data security and privacy policy that implements the requirements of Part 121 and aligns with the NIST Cyber Security Framework (CSF).

In addition to the above requirements, educational agencies are strongly encouraged to maintain a page on their websites devoted to privacy requirements, making data privacy and security information easily accessible, and transparent, to parents and eligible students. After monitoring by the Privacy Office, any educational agency that did not meet the requirements of Education Law § 2-d and Part 121 received a "Needs Work" letter and additional follow-up from the Privacy Office.

## VI. Enforcement

Education Law Section 2-d and 121.11 authorize the Chief Privacy Officer to investigate breaches or unauthorized releases of student data or teacher or principal data by third party contractors. If a violation of Education Law Section 2-d is determined, the Chief Privacy Officer is authorized to preclude the third party vendor from accessing PII or teacher or principal data for a limited amount of time, determine that the third party contractor is not a responsible bidder, require that the third party contractor undertake additional confidentiality training and/or assess penalties, among other requirements that the Chief Privacy Officer may deem appropriate in light of the nature of the breach or unauthorized release.
In 2024 the Chief Privacy Officer resolved the following enforcement matters:

- The College Board February 5, 2024
- Distributed Website Corporation (owner of rSchoolToday) August 7, 2024
- Raptor Technologies August 8, 2024

Agreements resulting from enforcement actions conducted pursuant to Education Law Section 2-d can be found on the NYSED Data Privacy and Security website.

## Conclusion

This report, previous annual reports, the Parents' Bill of Rights, information on how to file a complaint and complaint determinations, information on student privacy and Education Law § 2-d, as well as enforcement case determinations can be found on NYSED's data privacy and security web page.