New York City Public Schools

Privacy and Security of Student Data

Report 2023-N-6 | April 2026

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller
Division of State Government Accountability

Audit Highlights

Objective

To determine if the New York City Public Schools (NYCPS) consistently followed all laws and regulations regarding the privacy and security of students' data. The audit covered the period from March 2020 through September 2025.

About the Program

NYCPS, previously known as the New York City Department of Education, is the largest school district in the United States. NYCPS is considered one district for State Education Department (SED) reporting purposes. In school year 2024–25, there were approximately 1,600 schools and over 900,000 students within NYCPS. NYCPS uses Automate the Schools (ATS) as its main student information system (SIS), which standardizes and automates the collecting and reporting of student data. In total, ATS holds approximately 5 million records collected since it was implemented in 1984.

NYCPS maintains and uses students' personally identifiable information[1] (PII) for a variety of educational purposes. NYCPS is responsible for safeguarding student data and ensuring the confidentiality, integrity, and availability of its information systems. NYCPS is required to comply with federal privacy laws, including the Family Educational Rights and Privacy Act (FERPA). FERPA affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of PII from the education records.

NYCPS must also comply with section 2-d of the New York State Education Law (Law) and Part 121 of the Regulations of the Commissioner of Education (Part 121). The Law requires the Commissioner of Education to establish standards for data security and privacy policies. In accordance with the Law, Part 121 further strengthens data privacy and security by requiring schools to adopt and publish a data security and privacy policy that implements the requirements of Part 121 and aligns with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 1.1 by October 2020. NIST CSF is a comprehensive framework designed to help organizations of all sizes and sectors—including industry, government, academia, and non-profit—to manage and reduce their cybersecurity risks.

Key Findings

NYCPS can take steps to increase controls over the privacy and security of student data and strengthen its overall security posture. Specifically, we found:

- NYCPS' policy does not fully align with NIST CSF. We found that certain fundamental areas related to data privacy and security are not covered or described in NYCPS' policy. Furthermore, in some instances, not only is this information not published to its website, but NYCPS does not have an existing policy. For example, NYCPS does not have written policies covering the areas of data classification, risk assessment, and backup and recovery.

1 PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to an individual, including but not limited to, the name or address of a student, parent, or a family member; a personal identifier, such as a student number; date of birth; or other information that, alone or in combination with other information, could identify a student.

- NYCPS does not always report breaches or notify affected parties within the required time frames. We reviewed 141 breaches or unauthorized data releases from January 5, 2023 through February 27, 2025 that NYCPS reported to SED.
  - We found NYCPS delayed reporting 48% (67 of 141) of breaches to SED and delayed notifying affected individuals and families about 11% (16 of 141) of breaches.
- NYCPS does not have a documented data classification policy. NYCPS officials stated they have their own data classification process and classify information as either confidential or protected. Officials also stated that student information and teacher evaluation data are classified as protected information, and any other sensitive non-public information is classified as confidential information—with protected information being a subset of confidential information. However, this is not a written policy. In the case of an information security incident, NYCPS may be unable to identify in a timely manner what, if any, sensitive and/or critical data was involved and may have been compromised.
- NYCPS does not maintain a comprehensive list of all applications used by each school. We surveyed all schools to determine if any schools used an electronic SIS other than the two central office systems. Of the 524 responding schools, 218 (42%) stated they used at least 70 different SIS applications, reflecting a decentralized and uncoordinated application usage. Without an accurate inventory of all software applications being used at each school, NYCPS does not have a clear understanding of its environment, the type of information being stored in these applications, and the various risks associated with the data.
- Part 121 requires all employees with access to PII to complete training on their data privacy and security responsibilities on an annual basis. Although NYCPS requires all employees to take the training, we found that in 2024, only 73% (117,763 of 161,337) of employees completed the training. However, NYCPS does not review the list of employees who have completed the training to verify that those who have access to PII have, in fact, completed the training.
- We identified weaknesses in technical controls that need to be corrected to ensure the selected NYCPS information systems and their associated data are not at risk.
- Throughout the audit, the audit team had difficulties obtaining information and setting up meetings with NYCPS, with some documentation requests taking over 5 months to fulfill, and meeting requests taking 2 months to be scheduled, despite repeated requests.

Key Recommendations

- Using the applicable NIST CSF, identify gaps or enhancements to improve overall security posture as required.
- Develop a mechanism to ensure that NYCPS always issues notifications of breaches or unauthorized release of PII within required time frames.
- Complete a written data and asset classification policy that applies to all current NYCPS systems and data and complete a data classification of all NYCPS data.
- Develop a mechanism to ensure all student information systems used at schools are accounted for.
- Implement a monitoring process that ensures all employees with access to PII complete data privacy and security training annually.

- Implement the recommendations detailed in the confidential draft report to strengthen technical controls over the selected systems reviewed.
- Improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

Office of the New York State Comptroller
Division of State Government Accountability

April 23, 2026

Kamar H. Samuels
Chancellor
New York City Public Schools
52 Chambers Street
New York City, NY 10007

Dear Chancellor Samuels:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for the tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *Privacy and Security of Student Data*. This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article III of the General Municipal Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Division of State Government Accountability

Contents

Glossary of Terms

Term	Description	Identifier
NYCPS	New York City Public Schools	*Auditee*
ATS	Automate the Schools	*Key Term*
Citywide Policies	Citywide Cybersecurity Program Policies and Standards	*Key Term*
FERPA	Family Educational Rights and Privacy Act	*Law*
GAGAS	Generally accepted government auditing standards	*Key Term*
Law	Section 2-d of the New York State Education Law	*Law*
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework	*Key Term*
Part 121	Part 121 of the Regulations of the Commissioner of Education	*Regulation*
PII	Personally identifiable information	*Key Term*
SED	State Education Department	*Agency*
SIS	Student information system	*Key Term*

Background

The education sector is an attractive target for threat actors. Schools and universities hold vast amounts of data, and cyberattacks appear to have grown steadily over the past several years. According to the federal Cybersecurity and Infrastructure Security Agency, adversaries target K–12 education systems mainly because they maintain extensive personal and financial data about students, teachers, school staff, and records. Yet most educational agencies lack the resources to implement a comprehensive cybersecurity program.

New York City Public Schools (NYCPS), previously known as the New York City Department of Education, is the largest school district in the United States. NYCPS is considered one district for State Education Department (SED) reporting purposes. In school year 2024–25, there were approximately 1,600 schools and over 900,000 students within NYCPS. NYCPS uses Automate the Schools (ATS) as its main student information system (SIS), which standardizes and automates the collecting and reporting of student data. In total, ATS holds approximately 5 million records since it was implemented in 1984.

NYCPS maintains and uses students' personally identifiable information[2] (PII) for a variety of educational purposes. NYCPS is responsible for safeguarding student data and ensuring the confidentiality, integrity, and availability of its information systems. NYCPS is required to comply with federal privacy laws, including the Family Educational Rights and Privacy Act (FERPA). FERPA affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of PII from the education records.

NYCPS must also comply with section 2-d of the New York State Education Law (Law) and Part 121 of the Regulations of the Commissioner of Education (Part 121). The Law requires the Commissioner of Education to establish standards for data security and privacy policies, which include, but are not limited to:

- Data privacy protections
- Data security protections, including data systems monitoring
- Data encryption
- Incident response plans
- Limitations on access to PII
- Safeguards to ensure PII is not accessed by unauthorized persons when transmitted over communication networks
- Application of all such restrictions, requirements, and safeguards to third-party contractors

2 PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to an individual, including but not limited to, the name or address of a student, parent, or a family member; a personal identifier, such as a student number; date of birth; or other information that, alone or in combination with other information, could identify a student.

In accordance with the Law, Part 121 further strengthens data privacy and security by requiring schools to adopt and publish a data security and privacy policy that implements the requirements of Part 121 and aligns with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 1.1 by October 2020. NIST CSF is a comprehensive framework designed to help organizations of all sizes and sectors—including industry, government, academia, and non-profit—to manage and reduce their cybersecurity risks.

Additionally, NYC Cyber Command issues Citywide Cybersecurity Program Policies and Standards (Citywide Policies). These policies include requirements that NYCPS and other covered organizations must comply with in areas including but not limited to inventory, encryption, identity management, and information management.

In recent years, vendors used by NYCPS fell victim to cyberattacks that resulted in students' personal information being hacked. For example, in late December 2021 to early January 2022, a security breach occurred in Illuminate, a software company that NYCPS used, which resulted in over a million NYCPS students' PII—such as name, date of birth, ethnicity, academic records, and school enrollment—being leaked. More recently, in January 2025, NYCPS became aware that PowerSchool, a vendor that certain schools used to provide an SIS, was hacked. In this instance, hackers accessed students' names and dates of birth.

Audit Findings and Recommendations

NYCPS can take steps to increase controls over the privacy and security of student data and strengthen its overall security posture. We found that certain fundamental areas related to data privacy and security are not covered or described in NYCPS' policy. Furthermore, in some instances, not only is this information not published to its website, but NYCPS does not have an existing policy. NYCPS does not always report breaches or notify affected parties within the required time frames and does not adequately monitor the completion of training to verify that employees who did not take the training do not have access to PII or were on leave.

We also found NYCPS does not have a written data classification policy, which in the case of an information security incident, could result in NYCPS being unable to identify in a timely manner what, if any, sensitive and/or critical data was involved and may be compromised. Further, because NYCPS does not maintain a comprehensive list of all applications used by each school, it does not have a clear understanding of its environment, the type of information being stored in these applications, and the various risks associated with the data.

In addition, we identified weaknesses in technical controls that need to be corrected to ensure the selected NYCPS information systems and their associated data are not at risk. Due to their confidential nature, we provided a detailed confidential draft report to NYCPS officials.

Data Privacy and Security Policies

Part 121 became effective on January 29, 2020, and required educational agencies to adopt and publish to their website their data privacy and security policy that implements the requirements of Part 121 and aligns with NIST CSF 1.1 no later than October 1, 2020. Part 121 also requires that each educational agency publish on their website a Parents' Bill of Rights for data privacy and security that complies with the Law. NYCPS does have a data privacy and security policy and a Parents' Bill of Rights adopted and published on its website. The website also has the contact information of NYCPS' Chief Privacy Officer and SED's Chief Privacy Officer, with whom parents or other parties could file complaints. However, NYCPS' policy does not fully align with NIST CSF 1.1. We found that certain fundamental areas related to data privacy and security are not covered or described in NYCPS' policy. Furthermore, in some instances, not only is this information not published to its website, but NYCPS does not have an existing policy.

We found NYCPS does not have written policies covering the areas of data classification, risk assessment, and backup and recovery. We also found that although NYCPS has an asset management policy and incident response plan, there is no mention of them published as a part of NYCPS' policy. While we acknowledge that certain policies in their entirety would not be posted to NYCPS' website due to security risks, NYCPS' policy should indicate such policies exist and provide other pertinent high-level information about the policy. For example, SED's Data Privacy and Security Policy notes that it has developed an Incident Response Policy and Plan to guide its response to data and cybersecurity incidents, and contains

information for when the plan must be updated, who it is communicated to, and that it must be protected from unauthorized disclosure or modification.

Part 121 does not expressly state that every aspect of NIST CSF 1.1 must be followed; rather, it only states that data privacy and security policies must align with NIST CSF. Additionally, NIST CSF does not set forth requirements that an educational agency must implement. It is a framework that can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations, or it can be focused on the delivery of critical services within an organization. Gaps within its security policies weaken NYCPS' security posture. Although NYCPS is not expressly required to implement every aspect of NIST CSF 1.1, it should formally evaluate the framework and identify gaps or enhancements that can be implemented to increase its overall security posture.

Data Incidents/Breach Reporting and Notification

Data incidents, or breaches, are the unauthorized acquisition, access, use, or disclosure of student, teacher, or staff data. The Law requires educational agencies to notify parents or eligible students of the unauthorized release of student data that includes PII in the most expedient way possible and without unreasonable delay. Further Part 121 requires educational agencies to notify the SED Chief Privacy Officer no more than 10 calendar days after discovery and affected individuals or families no more than 60 calendar days after discovery of the incident/breach.

We reviewed 141 breaches/unauthorized data releases NYCPS reported to SED from January 5, 2023 through February 27, 2025. We found there were delays in reporting breaches/unauthorized data releases to SED and sending notifications to affected individuals.

Delays in Reporting to SED

During the period, we found NYCPS delayed reporting 48% (67 of 141) of breaches to SED:

- 2023 – 62% (24 of 39)
- 2024 – 46% (37 of 80)
- Early 2025 (January and February) – 27% (6 of 22)

Delays ranged from 1 to 460 days, for example:

- In May 2022, a mother submitted safety transfer papers for her daughter that included a partially redacted behavioral incident report with the names and grade levels of four other students. The issue was discovered on May 1, 2022, but was not officially reported until August 14, 2023, resulting in a 460-day delay.

- In another incident, the principal gave a parent a sealed envelope containing a redacted report about her son's bullying incident. However, the principal failed to redact all references to other students, causing the parent to receive the names, grade levels, and—in some cases—the parents' names, phone numbers, and addresses of seven other students. The incident was discovered on November 14, 2022, but was reported on March 6, 2023, after a delay of 102 days.
- Another incident involved the parent coordinator of a school, who intended to send staff an update regarding a student's uncle's telephone number but accidentally emailed the parent listserv (a type of electronic mailing list software) instead. As a result, the email disclosed the student's name and the uncle's phone number. The incident occurred on January 8, 2024, but was reported on June 10, 2024, after a delay of 144 days.

Delays in Reporting to Affected Individuals and Families

We also found delays in notifications to affected individuals and families. During the period, NYCPS delayed notifying individuals or families of 11% (16 of 141) of breaches:

- 2023 – 28% (11 of 39)
- 2024 – 3% (2 of 80)
- Early 2025 (January and February) – 14% (3 of 22)

Notification delays ranged from 3 to 400 days, for example:

- An incident occurred when a principal provided a parent with a partially redacted behavioral report, unintentionally leaving a student's name visible. The backside of the report contained immunization records for two additional students, exposing their personal data. The incident occurred on March 1, 2023, but the families were not informed of the disclosure until June 6, 2023, 97 days after discovery and 37 days after the required notification time frame.
- Another incident occurred on May 1, 2022 when an assistant principal provided a behavioral incident report to the family of a child that included the names and grade levels of four other students. The families of the affected students were notified on August 4, 2023, 460 days after discovery, and 400 days after the required notification time frame.

NYCPS has not established an adequate mechanism to ensure that it always sends notifications of breaches or unauthorized release of PII within required time frames. With the rise of cyberattacks, the timely communication of information is especially important. NYCPS should ensure that it completes notification to affected parties of data incidents within the time frames established in Part 121. Without accurate, timely notifications of data incidents, there could be a delay in the affected parties taking action to protect themselves. Further, delays in notifications to SED could result in delayed notification to other school districts that may use the same vendor.

Data Classification

Data classification is the basis for identifying an initial baseline set of security controls for data, data systems, and evaluation of retention and disposition schedules. Following a written data classification policy is extremely important, as it serves to protect sensitive information as well as ensure compliance with regulations. A typical data classification policy outlines how data will be classified, typically within criteria such as sensitivity or importance, as well as how to use these classifications to mitigate risks. A written data classification policy allows security controls to be placed on data based on its classification, which helps maintain the integrity of the data as well as ensure there is no unauthorized access to said data.

According to NIST CSF, resources such as data should be prioritized based on their classification, criticality, and business value. Data that enables an organization to achieve business purposes should be identified and managed consistent with its relative importance to business objectives and the organization's risk strategy. NYCPS does not have a documented data classification policy. Although NYCPS is a covered organization, it is exempt from NYC's Identifying Information Law, which includes the Citywide Data Classification Standard (Data Classification Standard). The Data Classification Standard details how information should be classified as either restricted, sensitive, or non-restricted. The Data Classification Standard also states that PII must be classified as either sensitive or restricted, except where the agency's privacy officer or the City's Chief Privacy Officer determines such classification is not required.

NYCPS officials stated that they have their own data classification process and classify information as either confidential or protected. Officials also stated that student information and teacher evaluation data is classified as protected information, and any other sensitive non-public information is classified as confidential information, with protected information being a subset of confidential information. However, this is not a written policy.

NYCPS has not dedicated sufficient resources toward completing a data and asset classification policy. NYCPS systems capturing, storing, or otherwise processing sensitive data that has not been classified could lack the appropriate security controls, and could potentially be accessed for unauthorized purposes or by unauthorized individuals. In the case of an information security incident, NYCPS may be unable to identify in a timely manner what, if any, sensitive and/or critical data was involved and may be compromised.

Student Information System Applications

An accurate software inventory is crucial for ensuring security, compliance, cost control, and operational efficiency. It enables organizations to identify vulnerabilities, manage software licenses correctly, reduce waste from unneeded software, and make informed IT decisions, ultimately protecting sensitive data and optimizing resource allocation. NIST CSF states that every organization should maintain a

comprehensive and accurate inventory of all software platforms and applications to ensure effective cybersecurity risk management. Further, Citywide Policies on inventory management require that agencies establish and maintain accurate and up-to-date inventories of systems, software, non-computing storage devices, and user accounts.

Under FERPA and the Law, NYCPS may disclose student information without consent to authorized third parties that have entered into written agreements with NYCPS and meet certain requirements. The third parties NYCPS has written agreements with include software providers, community-based organizations, researchers, and related service providers. Third parties only receive the types of student information agreed upon in the written agreement, for the schools or students that have requested to use their products or services, and only as necessary for the provision of those products or services.

NYCPS officials stated that they do not maintain a comprehensive list of all applications used by each school. We surveyed all schools and asked each school if it used any electronic system other than the two known central office systems (ATS and the Student Transcript and Academic Reporting System [STARS]). Of the 524 responding schools, 218 (42%) stated they used at least 70 different SIS applications, reflecting decentralized and uncoordinated application usage.

NYCPS officials stated the survey questions did not provide any definition for SIS, and school principals might not have had the technological knowledge to understand the difference between SIS and other off-the-shelf applications or systems and could have categorized these applications as SIS when they are not. NYCPS officials also stated that most of the identified 70 different systems are third-party systems purchased by schools and used for learning management or communication purposes. However, our survey question explicitly put into context the type of systems we were asking about. Overall, NYCPS lacks centralized oversight and formal tracking mechanisms for school-level application procurement. For example, NYCPS officials were unable to identify which schools used PowerSchool and who was affected by the breach.

Without an accurate inventory of all software applications being used at each school, NYCPS does not have a clear understanding of its environment, the type of information being stored in these applications, and the various risks associated with the data. Additionally, NYCPS does not know if these schools have entered into written agreements with the third-party vendors that host these applications. Furthermore, NYCPS risks an ineffective response to data breaches, potentially missing statutory notification deadlines and damaging its reputation.

Training

According to NIST CSF, an organization's personnel and partners should be provided cybersecurity awareness education and be adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Part 121 requires educational agencies

to provide data privacy and security awareness training annually to their officers and employees with access to PII. This training should include, but not be limited to, training on the State and federal laws that protect PII and how employees can comply with such laws.

NYCPS requires all employees—not only those with access to PII—to complete training on their data privacy and security responsibilities on an annual basis. Supervisors are responsible for ensuring their staff members complete their training. In 2024, only 73% (117,763 of 161,337) employees completed the training. NYCPS officials stated that individuals who did not take the training could include those who do not need to because they do not have access to student data, and those who have temporarily (sabbatical, medical leave) or permanently left. NYCPS officials monitor the overall completion of the training and send reminders to those who have not completed the training. However, NYCPS does not review the list of employees who have completed the training to verify that those who have access to PII have, in fact, completed the training.

If employees are not adequately trained in how to handle PII, it increases the risk that they will do something inappropriate with PII and potentially release student data to someone who should not have access to it.

Weaknesses in Technical Controls

During our testing, we identified weaknesses in technical controls that need to be corrected to ensure the selected NYCPS information systems and their associated data are not at risk. These included issues with system monitoring, unsupported systems, and firewalls. Due to their confidential nature, we disclosed these matters to NYCPS officials in a separate confidential draft report and, consequently, do not address them in detail in this report.

NYCPS Cooperation

We perform our audits under generally accepted government auditing standards (GAGAS), which require us to obtain sufficient, appropriate evidence to support our audit findings. As part of that, we need to evaluate the reliability of that evidence and whether circumstances adversely affect our ability to comply with GAGAS. A scope limitation, such as restrictions on access to records or people or excessive delays, would be considered a significant constraint that could potentially affect our ability to comply with GAGAS. Throughout the audit, the audit team had difficulties obtaining information and setting up meetings with NYCPS, with some documentation requests taking over 5 months to fulfill, and meeting requests taking 2 months to schedule, despite repeated requests. For example, the audit team requested a listing of data breaches in March 2024. Despite repeated follow-up requests, the information was not received until August 2024. Further, the audit team requested its first overview meeting in November 2023, but NYCPS officials did not schedule a meeting until January 2024. Due to the difficulties in receiving information, the audit team issued a scope impairment preliminary for access to data and key personnel to NYCPS on August 27, 2024.

Recommendations

1. Using the applicable NIST CSF, identify gaps or enhancements to improve overall security posture as required.
2. Develop a mechanism to ensure that NYCPS always issues notifications of breaches or unauthorized release of PII within required time frames.
3. Complete a written data and asset classification policy that applies to all current NYCPS systems and data and complete a data classification of all NYCPS data.
4. Develop a mechanism to ensure all SIS used at schools are accounted for.
5. Implement a monitoring process that ensures all employees with access to PII complete data privacy and security training annually.
6. Implement the recommendations detailed in the confidential draft report to strengthen technical controls over the selected systems reviewed.
7. Improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

Audit Objective, Scope, and Methodology

The objective of our audit was to determine if NYCPS consistently followed all laws and regulations regarding the privacy and security of students' data. The audit covered the period from March 2020 through September 2025.

To accomplish our objective and assess related internal controls, we reviewed relevant laws, regulations, and guidance. We interviewed NYCPS officials to gain an understanding of their efforts to monitor compliance with the requirements of Part 121. We also interviewed officials from multiple NYCPS program units to identify systems that handle student data and how NYCPS ensures compliance with Part 121. Further, we reviewed policies and procedures that we deemed important to the control, security, and maintenance of these systems. Additionally, we surveyed NYCPS school officials to determine what they do on the school level to ensure student data privacy. We also reviewed records and reports related to data breaches or unauthorized access incidents.

We obtained data from the Location Code Generation and Management System. We assessed the reliability of this data by comparing it to other publicly available information. We also obtained breach reporting data in the form of an Excel spreadsheet kept by SED. We assessed the reliability of this data by tracing pertinent information to source documents. We determined that the data obtained was sufficiently reliable for the purposes of this report.

Statutory Requirements

Authority

The audit was performed pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article III of the General Municipal Law.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. Even with the significant constraints NYCPS officials placed on our access to data (as discussed in the body of the report), we believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

As is our practice, we notify agency officials at the outset of each audit that we will be requesting a representation letter in which agency management provides assurances, to the best of their knowledge, concerning the relevance, accuracy, and competence of the evidence provided to the auditors during the audit. The representation letter is intended to confirm oral representations made to the auditors and to reduce the likelihood of misunderstandings. Agency officials normally use the representation letter to affirm that, to the best of their knowledge, all relevant financial and programmatic records and related data have been provided to the auditors. They further affirm either that the agency has complied with all laws, rules, and regulations applicable to its operations that would have a significant effect on the operating practices being audited, or that any exceptions have been disclosed to the auditors. However, officials at the New York City Mayor's Office of Operations informed us that, as a matter of policy, mayoral agencies do not provide representation letters in connection with our audits. As a result, we lack assurance from NYCPS officials that all relevant information was provided to us during the audit.

Reporting Requirements

We provided a draft copy of this report to NYCPS officials for their review and comment and considered their comments in preparing this final report. We have included their response in its entirety at the end of this report. In their response, NYCPS officials generally agreed with our audit conclusions and recommendations and have indicated actions planned or already ongoing to implement our recommendations. However, we added State Comptroller's Comments embedded within their response in several areas for clarification.

Within 180 days after final release of this report, as required by Section 170 of the Executive Law, the Chancellor of the New York City Public Schools shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

NYC Public Schools
Chancellor Kamar Samuels

March 10, 2026

Thomas P DiNapoli
State Comptroller
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th floor
Albany, NY 12236

Re: NYCPS Privacy and Security of Student Data (2023-N-6)

Dear Mr. DiNapoli:

This letter constitutes the formal response of the New York City Public Schools (NYCPS) to the recommendations made by the Office of the New York State Comptroller (Comptroller) in its draft audit report on NYCPS Privacy and Security of Student Data (Report).

Protecting the privacy and security of student data is of the utmost importance to NYCPS. NYCPS complies with all federal, state, and local privacy laws, including the Family Educational Rights and Privacy Act (FERPA), New York State Education Law § 2-d (Ed Law 2-d), and NYCPS Chancellor's Regulation A-820. To ensure compliance with these laws, NYCPS staffs a dedicated Student Privacy Office to counsel NYCPS schools and offices on best privacy practices.

In addition, NYCPS has instituted a rigorous data privacy compliance process to ensure that all third-party contractors that access student data do so safely and securely. The process requires that all such third-party contractors (i) enter into a data-processing agreement with NYCPS that ensures the confidentiality and security of student data, (ii) pass a thorough security review conducted by the NYCPS Division of Instructional and Information Technology (DIIT), and (iii) pass a separate security review conducted by the New York City Office of Technology and Innovation (OTI) for applications that store data in the cloud. Only those vendors that complete this process are approved for use at NYCPS.

Of course, data privacy obligations are only effective insofar as NYCPS staff are aware of them. To that end, NYCPS requires all employees to complete annual student privacy training. The Student Privacy Office also offers specialized training to meet the unique needs of different offices, as well as professional development sessions dedicated to student privacy. Student privacy

guidance is posted on the NYCPS website and disseminated via Principal's Digest and Superintendent's Digest, weekly newsletters distributed to school principals and superintendents, respectively.

In the past year alone, NYCPS has made several improvements to its privacy practices and policies. Chancellor's Regulation A-820 was updated to codify key provisions from Ed Law 2-d, restrict the use of "directory information," and make it easier for parents to exercise their right to access education records. NYCPS also created a new student privacy webpage[1] to better inform parents and students of their privacy rights and NYCPS' privacy practices. To better engage with the school community at large, NYCPS convened a data privacy working group comprised of school leaders, parents, advocates, and industry experts to solicit feedback with the goal of continuously improving student privacy at NYCPS.

State Comptroller's Comment – We are pleased that while our audit was ongoing, NYCPS proactively made improvements to its privacy practices and policies. We would have provided the details of these actions in our report; however, NYCPS officials did not share the majority of these ongoing efforts with the audit team. Chancellor's Regulation A-820 was updated in May 2025; however, we were not made aware that this update was taking place until June 2025, when our findings were issued to NYCPS about its data policies—despite the update being ongoing for months before that and directly affecting the audit. In fact, we asked NYCPS officials at the opening conference if there were any recent developments that would affect the audit objective and nothing was shared. Throughout the audit process, we also asked NYCPS to share details about its data privacy and security practices; however, again, this information was not shared. Under the U.S. Government Accountability Office's Government Auditing Standards, audited entities have a responsibility to provide auditors with timely, complete, and accurate information to support the audit process. When an auditee withholds information that is relevant and material to the audit, despite multiple opportunities to provide it, and later introduces that information in its formal response, it is inconsistent with the principles of transparency, cooperation, and full disclosure. As this is not an isolated incident, we encourage NYCPS to demonstrate meaningful improvement in transparency and timeliness in future audit engagements.

In the spirit of continuous improvement, NYCPS has accepted most of the recommendations in the Report, to the extent they have not already been implemented. There are, however, some claims and findings in the Report that should be clarified:

- The Report states that 281 charter schools are included in NYCPS. Charter schools and their data privacy and security practices are not governed by NYCPS.

  State Comptroller's Comment – We revised our final report and removed all references to charter schools.

[1] https://schools.nyc.gov/studentprivacy

- The Report states that in the December 2024 Power School data breach[2], hackers accessed students' Social Security numbers. No NYCPS students' Social Security numbers were accessed in that breach.

  State Comptroller's Comment – Our reference to the PowerSchool data breach was not meant to indicate that NYCPS' students' Social Security numbers were accessed. It was reported by PowerSchool that, during the breach, hackers accessed student's names, dates of birth, and Social Security numbers, but that the information access varied across different customers. The final report is edited for clarity.

- On p. 13 of the Report, it states that ". . . NYCPS officials were unable to identify which schools used Power School and who was affected by the breach." On the contrary, NYCPS quickly identified the four schools that used the impacted Power School application (Power School SIS) and notified the impacted families. It is unclear whether the Report's erroneous finding was based on the Comptroller Student Information System (SIS) survey, discussed below, which identified 19 schools that used Kinvolved, a Power School application that was not impacted by the breach.

  State Comptroller's Comment – Our conclusions and findings are based on communication with NYCPS management. In an email correspondence from February 2025, we asked NYCPS officials about the PowerSchool breach and what schools were affected. A member of NYCPS Executive Management responded and provided the four schools that were affected in the breach. He also stated that NYCPS received a notification of the breach from PowerSchool that stated NYCPS wasn't affected. However, NYCPS reached out to each school and asked if it received a notification from PowerSchool, and four had. The statement "... NYCPS officials were unable to identify which schools used PowerSchool and who was affected by the breach" was used in our report as an example to demonstrate the preceding sentence, "NYCPS lacks centralized oversight and formal tracking mechanisms for school-level application procurement." It was also used to support the overall finding that NYCPS does not know what applications are being used by each school, particularly SIS applications. The fact that NYCPS had to reach out to individual schools to find out if they were affected by the PowerSchool breach supports that conclusion and it is in no way erroneous. Further, when we asked NYCPS Executive Management if any other schools were affected, they were unable to tell us. They responded, "We don't have that information. Schools retain a degree of discretion over what products they choose to purchase and use, and DOE [CPS] does not centrally track which products each individual school uses."

- The Report on p. 13 refers to the survey conducted by the Comptroller that revealed "[o]f the 524 responding schools, 218 (42%) responded stating they used at least 70 different SIS applications[3] reflecting decentralized and uncoordinated application usage."[4] The

[2] The data breach impacted only one Power School application, Power School SIS. NYCPS posted information about the incident on its website at https://www.schools.nyc.gov/about-us/policies/data-privacy-and-security-policies/data- security-incidents.

[3] The research and advisory firm Gartner defines SIS as follows: "The student information system of the typical K-12

Comptroller only shared a portion of the survey responses with NYCPS, and those responses included applications that are not SIS applications. For example, Kinvolved is a Power School application that tracks daily attendance and supports communication between schools and families. It is not an SIS. Nor are Insight Education (a college admissions application), JumpRope (a learning management system), or Operoo (an operations and productivity platform). The Report acknowledges NYCPS' objections to the survey, specifically that it failed to define "SIS," leading to responses that included non-SIS applications.[5] Yet the Comptroller nevertheless continues to classify each of these applications as a SIS application in its Report. Furthermore, NYCPS also confirmed that all 70 applications referenced completed the ERMA security review process, showing that third-party tools used by schools—including tools that may use student data—are reviewed and approved by NYCPS security, privacy, and technical staff.

State Comptroller's Comment – Under NYCPS policy, any application functioning like a SIS must obtain central approval before it can be adopted by a school. This helps prevent risks such as data breaches, unauthorized data sharing, and fragmented systems that undermine oversight, accountability, and effective governance. This survey was used to demonstrate that NYCPS does not know the applications that each individual school uses and, therefore, does not know whether schools are using applications such as SIS that can put student data at risk. In June 2025, we provided the details of the survey to NYCPS as requested. We also accurately reported the results of the survey to reflect how the schools responded. In their response, NYCPS officials focus on pointing out that several applications identified by school district personnel as SIS applications are not, in fact, SISs; however, rather than detracting from the finding, it further reinforces the conclusion reached. Schools that responded to the survey do not have a good understanding of the systems they are using and, thus, the potential risks. Moreover, NYCPS does not know what applications are being utilized by each individual school within its district—even SIS applications—and, therefore, is limited in its ability to mitigate the risk of these applications if a problem occurs.

organization continues to sit at the center of nearly all its data management. It provides back-office administrator functionality, as well as student-, parent- and faculty-facing functionality to manage key organizational information assets. Such assets include not only demographic data, enrollment, grades, and transcripts, but also state or other governmental agency reporting capabilities. Systems vary widely in size; scope; state, regional or national markets; and functional capability — and they range from individual components to enterprise-wide integrated solutions. They also function as the system of record for several other critical applications, including the LMS, demanding interoperability." https://www.gartner.com/en/information-technology/glossary/k-12-student-information-systems. NYCPS uses Automate the Schools (ATS), an on-premises platform, as its primary SIS.

[4] While ambiguous, NYCPS understands this finding to mean that OSC identified a total of 70 applications used across 218 schools, not that each school used at least 70 different applications.

[5] Other than the identification of the school, the only survey question shared with NYCPS was: "Has your school used any electronic Student Information System aside from ATS and STARS from January 2020 to the present?". STARS is an on-premises application used by NYCPS to standardize and automate the collection and reporting of academic data for NYC public schools. STARS Admin is an on-premises application used for course scheduling and grade management.

Response to Recommendations

Recommendation 1.: *Using the applicable NIST CSF, identify gaps or enhancements to improve overall security posture as required.*

Response. NYCPS agrees with this recommendation in that it is consistent with current practices and policies.

NYCPS will continue to implement the NIST CSF to assess its cybersecurity posture and identify areas for enhancement.

Recommendation 2. *Develop a mechanism to ensure that NYCPS always issues notifications of breaches or unauthorized release of PII within required time frames.*

Response. NYCPS agrees with this recommendation in that it is consistent with current practices and policies.

All NYCPS employees are instructed to immediately report unauthorized disclosures to the Student Privacy Office, which in turn reports the unauthorized disclosure to the New York State Chief Privacy Officer in accordance with Ed Law 2-d. Admittedly, the Student Privacy Office does not always receive these reports immediately following the unauthorized disclosure. NYCPS will look to improve its guidance to staff, including the mandated student privacy training, to improve the timeliness of reporting unauthorized disclosures to the State.

There are additional challenges when unauthorized disclosures result from a large-scale data breach of a third-party vendor. In these situations, third-party vendors typically conduct a forensic investigation to identify the impacted data. As a result, NYCPS must wait until the investigation is concluded before it can obtain from the third-party vendor the data necessary to effectuate detailed notifications, which, pursuant to 8 N.Y.C.R.R. 121.10(g), include, among other things, a description of the breach or unauthorized release, date(s) of the incident, a description of the personally identifiable information affected, and the estimated number of records affected. Once NYCPS receives that data, it must match it against its own databases to ensure notifications are sent to the appropriate recipients and, pursuant to Chancellor's Regulation A-663, translate the notices into the recipient's home language. These factors—all of which are necessary to ensure impacted individuals are appropriately notified—often put NYCPS up against the statutory notification deadline. Nevertheless, NYCPS will endeavor to enhance its processes to improve the timeliness of its notifications to impacted individuals.

Recommendation 3. *Complete a written data and asset classification policy that applies to all current NYCPS systems and data and complete a data classification of all NYCPS data.*

Response. NYCPS agrees with this recommendation.

NYCPS currently classifies data as "Confidential" (or "Restricted" under the Citywide Data Classification Standard[6]), "Sensitive" (also "Sensitive" under the Citywide Data Classification Standard), and "Public" (also "Public" under the Citywide Data Classification Standard). While these designations are documented in NYCPS guidance and in its agreements with third-party vendors, NYCPS will adopt this recommendation and draft an updated data classification policy and apply it to NYCPS data.

Recommendation 4. *Develop a mechanism to ensure all SIS used at schools are accounted for.*

Response. NYCPS agrees with this recommendation to the extent that it is consistent with current practices and policies.

The Report on p. 13 concludes that "[o]verall, NYCPS lacks centralized oversight and formal tracking mechanisms for school-level application procurement." To the contrary, NYCPS requires that any software application that processes student data, including student information systems (SIS), pass a data privacy and compliance review before use.[7] Only after an application passes this review process will it be listed as "approved" in the Enterprise Request Management Application (ERMA), a centralized database that indicates whether a particular product or service has been approved for use with student data. The ERMA approval status is also integrated into centralized purchasing systems—which schools must use when purchasing software applications—to ensure that only those products that are listed as approved in ERMA are available for purchase by NYCPS schools or offices. Using these centralized systems, NYCPS is able to determine which SIS or other applications that consume student data are in use by a given school or office.

State Comptroller's Comment – As discussed in our State Comptroller's Comment above, NYCPS was unable to determine which schools used PowerSchool without asking each school. Further, when we asked NYCPS Executive Management if any other schools were affected, they were unable to tell us. They responded, "We don't have that information. Schools retain a degree of discretion over what products they choose to purchase and use, and DOE [CPS] does not centrally track which products each individual school uses." Therefore, while NYCPS approves what applications can be used district-wide, it is unable to determine which SISs or other applications that contain student data each individual or specific school is using. NYCPS should implement a process to determine what application each individual school and/or unit utilizes.

[6] Available at https://cityshare.nycnet/intranets/cityshare_home/assets/cityshare_home/downloads/pdf/it-telecom/information-security-policies/S-01-PR-DS_Citywide_Data_Classification_Standard-Sensitive.pdf

[7] The data privacy and compliance process is described above and on the NYCPS website at https://infohub.nyced.org/in-our-schools/policies/data-privacy-and-security-compliance-process

Recommendation 5. *Implement a monitoring process that ensures all employees with access to PII complete data privacy and security training annually.*

Response. NYCPS agrees with this recommendation to the extent that it is consistent with current practice and policies.

All NYCPS employees are required to complete annual data privacy and security training. NYCPS tracks training completion and issues reminders and follow-up communications to employees who have not completed the training by the initial deadline.

NYCPS does not categorize employees based on whether they have access to student data. For this reason, NYCPS requires all employees to complete the training, which ensures that individuals with access to PII are included. This approach reflects the scale and operational realities of NYCPS as a large, decentralized organization with over 150,000 employees, where job assignments, duties, and related system access can change throughout the year (including temporary coverage and role changes). In that environment, maintaining an always-current, definitive list of *individuals* with access to student records is not only administratively complex, but also presents an under-inclusion risk—*i.e.,* a risk that someone whose role changes mid-year (or who is granted temporary access) could be omitted from a static roster. Accordingly, NYCPS takes a conservative compliance approach by offering training to the full workforce annually, rather than relying on a potentially incomplete classification scheme.

NYCPS will continue to explore additional mechanisms to increase completion rates for its annual data privacy and security training.

State Comptroller's Comment – It is irrelevant that NYCPS requires all employees to complete privacy and security awareness training annually. In 2024, more than 25% of employees did not complete the training. If any of these employees had access to PII, NYCPS is not in compliance with Part 121. Further, if NYCPS is not going to implement a process that ensures all employees who have access to PII actually complete the training, it will not be in compliance with Part 121.

Recommendation 6. *Implement the recommendations detailed in the confidential draft report to strengthen technical controls over the selected systems reviewed.*

Response. The response related to this recommendation has been incorporated into the confidential draft report, where it is being addressed through the appropriate secure process.

Recommendation 7. *Improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.*

Response. NYCPS respectfully disagrees with the conclusion underlying this recommendation.

At the outset of the audit, NYCPS outlined its established process for coordinating external oversight requests, which is designed to promote accuracy, consistency, and appropriate protection of confidential student and personnel information. That process was consistently followed throughout the engagement.

NYCPS devoted substantial staff resources to supporting the audit, including senior leadership and subject matter experts across multiple divisions. As the largest public-school system in the nation, NYCPS must balance audit support with ongoing operational responsibilities necessary to maintain uninterrupted services for students and families. In some instances, record production required cross-divisional coordination, legal review, and data validation to ensure completeness and compliance with applicable privacy laws and regulations.

NYCPS remains committed to transparent and accountable operations and to cooperating fully with *all* authorized oversight inquiries. However, NYCPS does not agree that the audit identified systemic timeliness concerns that would warrant this recommendation.

State Comptroller's Comment – As described in our report, during our audit, we faced excessive delays obtaining information and scheduling meetings—with some documentation requests taking over 5 months to fulfill, and meeting requests taking 2 months to schedule, despite repeated requests. This length of time to fulfill these requests is unacceptable and had a significant impact on the time it took for us to complete our audit. Further, we suggested multiple other approaches to prevent these unnecessary delays, but NYCPS refused to change its process. Additionally, as described in our first State Comptroller's Comment, NYCPS officials did not disclose important details about improvements they were implementing during our audit, further demonstrating their lack of transparency and cooperation.

Sincerely,

Kevin Moran
Deputy Chancellor of School Operations

Contributors to Report

Executive Team

Andrea C. Miller - *Executive Deputy Comptroller*
Tina Kim - *Deputy Comptroller*
Stephen C. Lynch - *Assistant Comptroller*

Audit Team

Nadine Morrell, CISM - *Audit Director*
Amanda Eveleth, CFE - *Audit Manager*
Justin Dasenbrock, CISA, ITIL, CC - *IT Audit Manager*
Daniel Raczynski - *IT Audit Manager*
Vito Gentile - *IT Audit Supervisor*
Misty Baldeo - *Information Systems Auditor*
Ingrid Qian - *Information Systems Auditor*
Taofeek Raheem, CISA - *Information Systems Auditor*
Stephen Kurtis - *Senior Examiner*
Rachel Moore - *Senior Editor*

Contact Information
(518) 474-3271
StateGovernmentAccountability@osc.ny.gov
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

For more audits or information, please visit: www.osc.state.ny.us/state-agencies/audits