New York State Comptroller
THOMAS P. DiNAPOLI

Charter School of Educational Excellence

Information Technology

2023M-174 | June 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Charter School of Educational Excellence

Audit Objective

Determine whether the Charter School of Educational Excellence (School) Board of Trustees (Board) and officials secured student data to help protect it from unauthorized access and developed and adopted a comprehensive information technology (IT) contingency plan.

Key Findings

The Board and officials did not adequately secure student data to help protect it from unauthorized access or develop an IT contingency plan. As a result, there was an increased risk of unauthorized access to student personal, private and sensitive information (PPSI) and personally identifiable information (PII), and that the School could suffer a serious interruption to operations since its ability to communicate during a disruption or disaster could affect the timely processing of its business functions. In addition to sensitive IT control weaknesses which we communicated confidentially to School officials, we found:

- School employees did not have guidance on how to properly identify and secure sensitive student data.
- Three out of six tested users of the cloud-based application used for School operations stored sensitive student data without adequate protection, and 12 of the 125 users of the cloud-based Student Information System (SIS) had excessive or unnecessary access to view and modify sensitive student data.

Key Recommendations

- Review, revise (if necessary), adopt and communicate the data classification policy to employees.
- Ensure all access to sensitive student data is based on needs and job responsibilities.
- Develop a written IT contingency plan.

School officials agreed with our recommendations and have initiated, or indicated they planned to initiate, corrective action.

Audit Period

July 1, 2021 – May 24, 2023

Background

The School is located in the City of Yonkers in Westchester County. The New York State (State) Board of Regents approved the School's charter in December 2003 and the School was opened in July 2005.

The seven-member Board is responsible for managing and controlling the School's financial and educational affairs. The Superintendent is responsible, along with other administrative staff, for the School's day-to-day management under the Board's direction.

The Superintendent designated the Director of Student Data (Director) as the Data Protection Officer (DPO), who is responsible for implementing data privacy and security policies and procedures and serves as the School's point of contact for data security and privacy.

The School has a Service Level Agreement (SLA) with an IT vendor to manage the School's day-to-day IT operations, including shared application folders and SIS, and ensuring appropriate IT contingency measures are in place and tested.

Quick Facts	
2022-23 Student Enrollment	1,127
Staff	130
IT Vendor SLA for 2022-23	$201,000

Information Technology

The School relies on its IT assets for maintaining student data, much of which contain PPSI[1] and PII,[2] and are accessed through shared application folders and a SIS application. School employees use these two cloud-based applications to access, store and share sensitive student and non-financial information. If shared application folder or SIS application access is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and rebuild. While effective controls, such as adequately secured shared application folder and SIS application access, will not guarantee the safety of student PPSI/PII accessibility and its storage in cloud-based applications, a lack of effective controls significantly increases the risk of unauthorized use, access, and loss of student PPSI/PII. In addition, an IT contingency plan can help prepare personnel for actions needed in the event of unauthorized use or loss of PPSI/PII, or other types of IT disruptions, and could help significantly reduce the resulting impact on the School's IT assets.

How Should the Board and School Officials Secure Student Data?

To help secure student data, the Board and School officials should require a data inventory or mapping that identifies software applications accessing data at various sensitivity levels and the School's IT assets that use those applications. The Board should also require that School officials develop data classification guidelines where data is assigned different levels of protection, such as "Sensitive," "Confidential" and "Public." User account access to shared application folders should also be secured to help safeguard any PPSI contained therein. To accomplish this, shared application folders should be setup to restrict access to only the user accounts of those who need the access to perform their assigned job duties.

Access controls define the users or computer processes that may have access to a specific IT resource, such as a software program, database or cloud-based application. For example, access controls can be implemented to limit who can view electronic files containing sensitive student data stored in shared application folders. School officials should implement adequate access controls by determining what level and type of protection is appropriate for various IT resources (e.g., data, cloud-based applications) and who needs access to those resources. Excessive access is when users are granted more access to electronic files containing sensitive student information than necessary based on their assigned job duties and responsibilities. For example, a user who only needs

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

[2] PII is any information which, because of names, numbers or other identifiers, can be used to identify a person.

access to print information should not have access to update, delete or modify the information. Unnecessary access is when users do not have compelling business reasons to have access to student data and the related application modules.

The School's Data Classification Privacy and Security Policy (Policy) required that officials monitor its data system and limit PII access to employees and third-party contractors who need the access to fulfil their professional responsibilities or contractual obligations. The Policy also requires that the School provides annual training on data privacy and security awareness to officers, teachers, staff and administrators who have access to PII related to students, teachers or principals. The Policy stated that training should include State and federal laws that protect PII, and how officers and employees should comply with such laws. In addition, the Policy requires that the Superintendent appoints a DPO who is responsible for the implementation of the policies and procedures. The Superintendent, in consultation with appropriate business and technology personnel, and DPO should establish policies which address:

- Protecting all student and staff PII,
- Protecting PII in accordance with State Technology Law, and
- Procedures to notify individuals affected by breaches or unauthorized access of protected information.

The Board and School Officials Did Not Adequately Secure Student Data

The Board and School officials did not adequately secure student data in the School's shared application folders and SIS. We obtained read-only access to the shared application folders of six employees and a listing of SIS user access rights of the 125 users with access to the application. We reviewed the shared application folders and SIS user access rights to determine whether student data was secured and access to the data was only assigned to users with a business need.

Shared Application Folders – Sensitive student data was not adequately secured in the shared application folders of three out of six employees we reviewed. The three employees stored sensitive and non-sensitive student information in their shared application folders. However, access to the sensitive student information was not restricted by measures to limit the access to only those who needed access to perform their assigned job duties and were granted permissions to sensitive student information. As a result, the folders were also accessible by other employees because no additional access permissions were required to help prevent unauthorized or unnecessary access.

This occurred because the Superintendent and DPO did not establish the additional policies that address the protection of all student PII in accordance with State Technology Law or develop breach or unauthorized access of protected information procedures as required by the Board-approved Policy. Because the Policy did not include data inventory or mapping procedures, School employees did not have guidance on how to properly identify sensitive student data. In addition, School employees did not know how to properly store sensitive student data by using data classification. Subsequent to audit fieldwork, the IT vendor provided a separate policy that included data classification guidelines. However, the policy was not adopted by the Board or communicated to employees.

Although the School provided IT security awareness training, it did not include procedures for data privacy or information on State and federal laws for protecting student PII and how employees should comply with such laws. As a result, student data was not secured because employees stored both sensitive student data and non-sensitive information in the same manner without additional requirements to access sensitive information in shared application folders.

SIS Application Access Permissions – We determined that 12 of the 125 SIS application users (10 percent) had unnecessary SIS access permissions to both view and modify sensitive student data. For example, three users had unnecessary access permissions to modify sensitive student data. The Director told us that these users needed the access for administrative tasks and to prepare, update and report student information to State agencies. However, view-only permissions should have been sufficient for these users, as their ability to modify access was unnecessary based on their assigned job duties and contractual responsibilities. Furthermore, a user who required access to view and modify student data changed positions. However, the access permissions were not removed after the change even though they were not necessary for the new position. The Director could not provide a reasonable explanation why the remaining eight users had access permissions to view and modify student data in the SIS.

Because the DPO did not adequately restrict access permissions within the SIS application or assign users to appropriate application modules, there were increased opportunities for users to access, view and improperly use sensitive student data and make unauthorized or improper changes. In addition, because the Board did not require the Superintendent to properly secure access to the shared application folders and adequately manage the SIS application access permissions, there was a significant risk that student information could be intentionally or unintentionally changed, shared or used inappropriately.

Why Should the Board and School Officials Develop and Adopt an IT Contingency Plan?

The Board and School officials should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of services in the event of an unexpected IT disruption or disaster. An IT contingency plan is a school's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT incident, such as a power outage, software failure caused by a ransomware or other type of malware infection, inadvertent employee action, equipment destruction or a natural disaster (e.g., flood or fire). Unplanned service interruptions are inevitable, and it is crucial to plan for such events.

The content, length and resources necessary to prepare an IT contingency plan vary depending on the size and sophistication of a school's computerized operations. Proactively anticipating and planning for IT disruptions helps prepare personnel for the actions they must take in the event of an incident. Because IT systems often support key business processes, planning for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining or recovering a school's critical business processes in the event of a disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Backup policies and procedures are also critical components and help ensure that information is routinely backed up and available in the event of a disruption. An IT contingency plan can also include, among other items deemed necessary by school officials, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the responsibilities of key personnel,
- Communication protocols with outside parties,
- Prioritized mission critical processes,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,
- Backup methods and storage policies, and
- Details concerning how the plan will be periodically tested and updated as needed.

The Board and School Officials Did Not Develop and Adopt an IT Contingency Plan

The Board and School officials did not develop and adopt an IT contingency plan to describe how officials should respond to potential disruptions and disasters affecting the School's IT systems. We requested the contingency plan to review and determine whether it met the School's needs, but officials did not provide a plan. The IT vendor, who is contractually responsible for ensuring appropriate contingency measures are in place, told us they are currently developing an IT contingency plan specifically designed for the School.

Without a comprehensive IT contingency plan that all key School officials have been trained on and is periodically tested for effectiveness, the Board has less assurance that officials and other responsible parties will react quickly and effectively to maintain business continuity. In addition, the Board cannot ensure the recovery of necessary data to continue operations if a system malfunction or other disruption occurs unexpectedly. As a result, important financial and other data could be lost or the School could suffer a disruption to operations that depend on the computerized environment.

What Do We Recommend?

The Superintendent should:

1. Work with the Board to review, revise (if necessary) and adopt the data classification policy and work with Director (as the DPO) to develop procedures for PPSI/PII and other sensitive student data.

2. Ensure annual training on data privacy, classification of data and security awareness is provided to officers, teachers, staff and administrators who have access to PII related to students, teachers or principals, as required by the School's Policy.

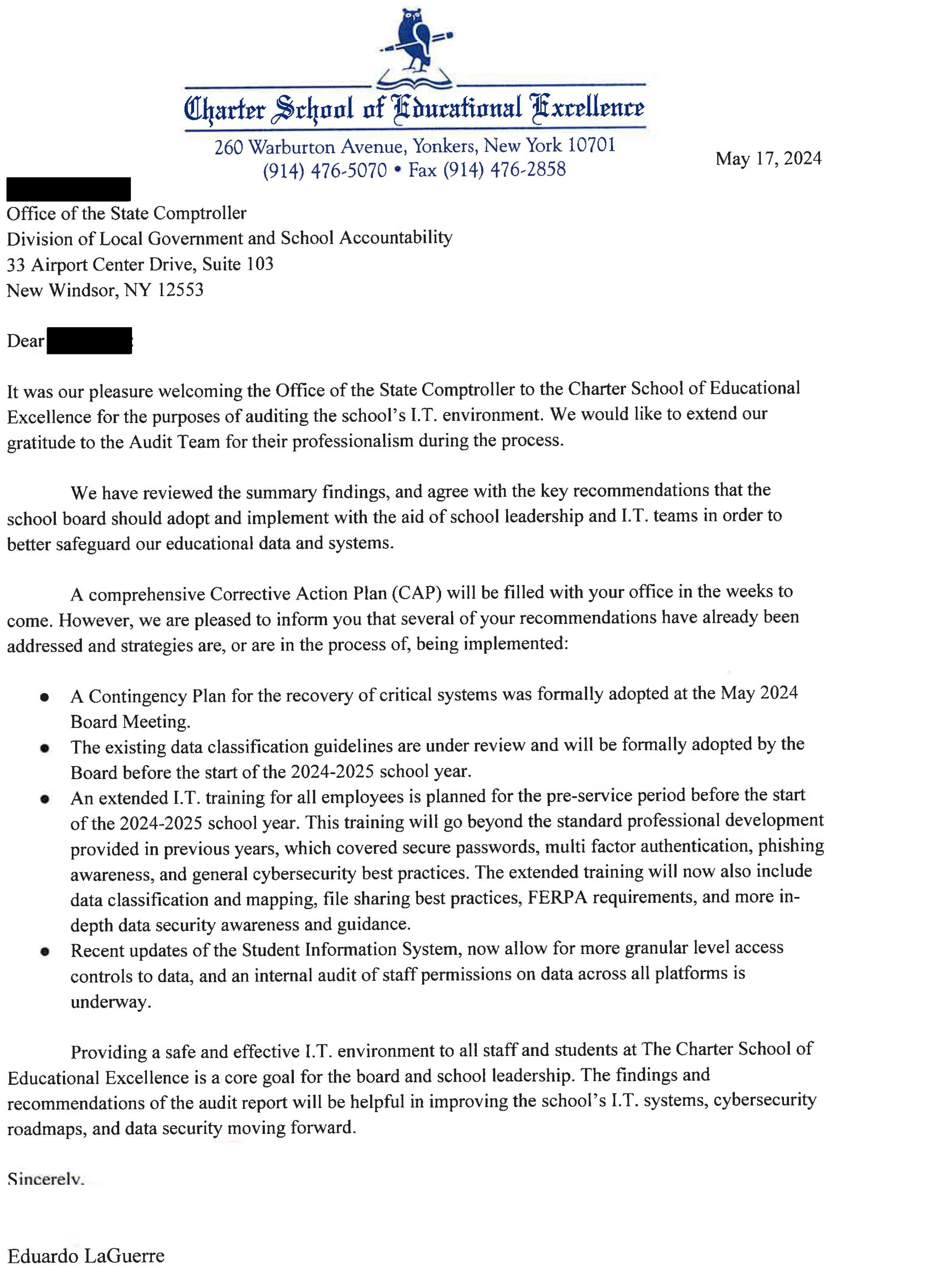
The Director should:

3. Ensure all access rights to the SIS and shared application folders housing sensitive student data are based on need consistent with assigned job duties and responsibilities, and the SIS access is limited to the appropriate application modules or groups.

The Board and School officials should:

4. Develop and adopt a comprehensive written IT contingency plan to address the School's specific needs, including backup procedures, update the plan as needed and distribute it to all responsible parties.

Appendix A: Response From School Officials



Charter School of Educational Excellence

260 Warburton Avenue, Yonkers, New York 10701
(914) 476-5070 • Fax (914) 476-2858

May 17, 2024

[redacted]
Office of the State Comptroller
Division of Local Government and School Accountability
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

Dear [redacted]

It was our pleasure welcoming the Office of the State Comptroller to the Charter School of Educational Excellence for the purposes of auditing the school's I.T. environment. We would like to extend our gratitude to the Audit Team for their professionalism during the process.

We have reviewed the summary findings, and agree with the key recommendations that the school board should adopt and implement with the aid of school leadership and I.T. teams in order to better safeguard our educational data and systems.

A comprehensive Corrective Action Plan (CAP) will be filled with your office in the weeks to come. However, we are pleased to inform you that several of your recommendations have already been addressed and strategies are, or are in the process of, being implemented:

- A Contingency Plan for the recovery of critical systems was formally adopted at the May 2024 Board Meeting.
- The existing data classification guidelines are under review and will be formally adopted by the Board before the start of the 2024-2025 school year.
- An extended I.T. training for all employees is planned for the pre-service period before the start of the 2024-2025 school year. This training will go beyond the standard professional development provided in previous years, which covered secure passwords, multi factor authentication, phishing awareness, and general cybersecurity best practices. The extended training will now also include data classification and mapping, file sharing best practices, FERPA requirements, and more in-depth data security awareness and guidance.
- Recent updates of the Student Information System, now allow for more granular level access controls to data, and an internal audit of staff permissions on data across all platforms is underway.

Providing a safe and effective I.T. environment to all staff and students at The Charter School of Educational Excellence is a core goal for the board and school leadership. The findings and recommendations of the audit report will be helpful in improving the school's I.T. systems, cybersecurity roadmaps, and data security moving forward.

Sincerely,

Eduardo LaGuerre

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Section 2854 of the New York State Education Law, as amended by Chapter 56 of the Laws of 2014. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed School officials, employees and the IT vendor and reviewed Board policies and meeting minutes to gain an understanding of the School's policies, procedures, practices and internal controls related to student data privacy and security, and managing user accounts and permissions in SIS and shared application folders.
- We requested the School's IT contingency plan to determine whether the plan existed, and if it adequately addressed the School's specific contingency concerns.
- We reviewed the IT training materials to determine whether they adequately addressed the annual training requirements on data privacy and security awareness stated in the School's Policy, and if they included training on the federal and State laws governing the confidentiality of PII and how to comply with those laws.
- We reviewed the School's contract with the IT vendor and SIS application consultant to determine whether the roles and responsibilities of each party were clearly stated and contract terms were reasonable.
- We examined the list of SIS application user accounts generated by the Director and determined that there were 125 unique users. We compared the 125 users to the Employee Master Listing to determine whether all users were current School employees. We asked the Director about the process of adding, modifying and deleting access permissions to the application. We reviewed SIS user access permissions to identify the type of permissions granted to School administrators, teachers and staff and determine whether the access was appropriate.
- We used our professional judgment to select the cloud-based shared application folders of six employees who had access to PPSI during the course of performing their assigned job duties and responsibilities and requested read-only access permissions to review the access to their shared application folders. We accessed the cloud application storage of each selected employee to search for PPSI key words, including highly sensitive student information.

- We followed up with School officials to gain an understanding of the cause for storing and potentially sharing sensitive student information on School systems or with external parties without limiting the access to those who needed the access to perform their job duties and responsibilities or enabling additional shared application folders' security features.

Our audit also examined the adequacy of certain sensitive IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to School officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. We encourage the Board to prepare a written corrective action plan (CAP) that addresses the recommendations in this report and forward it to our office within 90 days. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the School's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.ny.gov/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

https://www.osc.ny.gov/local-government

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief of Municipal Audits

33 Airport Center Drive, Suite 102 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties