New York State Comptroller
THOMAS P. DiNAPOLI

Discovery Charter School

Network and Financial Software Access Controls

2022M-156 | February 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Discovery Charter School

Audit Objective

Determine whether Discovery Charter School (School) officials ensured network and financial software access controls were adequate.

Key Findings

School officials did not ensure that network and financial software access controls were adequate. As a result, data and personal, private and sensitive information (PPSI) are at greater risk for unauthorized access, misuse, or loss. In addition to finding sensitive information technology (IT) control weaknesses, which we communicated confidentially to officials, we found that:

- Officials did not adopt adequate network and financial software policies, establish an IT contingency plan, or provide IT security awareness training.
- 18 percent of the School's enabled nonstudent user accounts were not needed, which created additional entry points for someone to inappropriately access the School's network.
- Two of the three financial software user accounts unnecessarily had full access, and three individuals unnecessarily shared access to a user account with administrative permissions. As a result, users could alter data and conceal inappropriate activity with limited ability for officials to trace the activity to a specific user.
- The IT service provider's contract did not define responsibilities. This can contribute to confusion over network responsibilities, which could expose the School's IT assets to risk for unauthorized access, misuse or loss.

Key Recommendations

- Properly manage network and financial software user accounts and establish adequate written policies for network and financial software access.

School officials agreed with our recommendations and indicated they will initiate corrective action.

Background

The School is located in the Town of Greece in Monroe County. The New York State Board of Regents approved the School's charter in December 2010.

The School is governed by an 11-member Board that is responsible for managing and controlling the School's financial and educational affairs. The School Director (Director) is responsible, along with other administrative staff, for the day-to-day management of the School under the direction of the Board.

The School contracts with a vendor to provide IT services, which includes managing network and financial software access controls. The IT service provider assigned three of its employees to the School, including an IT Manager, to provide IT services. The School's Operations Manager is responsible for overseeing the IT service provider.

Quick Facts

Enabled Network User Accounts	
Individual Non-Student	86
Service	21
Shared	18
Total	125
Reviewed	125
Financial Software	
Enabled User Accounts	3
2021-22 IT Service Provider	
Agreed Upon Cost	$90,922

Audit Period

July 1, 2020 – June 29, 2022

Network and Financial Software Access Controls

The School relies on its network and financial software for maintaining financial, student and personnel records, much of which contain personal, private and sensitive information (PPSI); accessing the Internet; and sending and receiving email. 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.

If the School's network or financial software access is compromised or disrupted, the results could range from inconvenience to significant damage and could require extensive effort and resources to evaluate, repair and/or rebuild. While effective network and financial software access controls will not guarantee the safety of these systems, without these controls the School has an increased risk that its network hardware, financial software and data contained therein, including PPSI, may be exposed, damaged or lost through inappropriate access and use.

How Can the Board and Officials Help Ensure There Are Adequate Network and Financial Software Access Controls?

By adopting written policies and procedures, a charter school (school) board of trustees (board) can help ensure adequate network and financial software access controls. Network and financial software access control policies should describe the tools to use and procedures to follow to help protect these systems and the data they contain, define appropriate user behavior when accessing the network and financial software and explain the consequences of policy violations.

A board should adopt written policies that address user accounts, passwords, remote access and audit trails, which are records of activity indicating who has accessed the network or financial software, the time and date of the access and what activity occurred. A board also must adopt a breach notification policy to ensure that affected parties are notified if unauthorized access of their private information occurs.

In addition, inadequate network and financial software access controls increase the risk of unauthorized access, which could lead to an unexpected disruption. Therefore, a board should adopt a written IT contingency plan containing procedures and technical measures that help enable the recovery of network and financial software operations after an unexpected disruption. The IT contingency plan should address, and establish controls for, how users will access the network and financial software, or its data, as quickly and effectively as possible to maintain school operations.

Without comprehensive written policies and procedures that explicitly convey a school's network and financial software access controls, officials cannot ensure that users are aware of their responsibilities for helping to protect these systems and the data they contain from unauthorized access, misuse and loss.

The Board and Officials Did Not Ensure There Were Adequate Network and Financial Software Access Control Policies

The Board adopted acceptable use policies that defined appropriate user behavior when accessing the network, but did not adopt other network and financial software access control policies. Specifically, School officials did not develop an IT contingency plan or policies related to:

- User account management, including adding or disabling user accounts on the network or in the financial software.
- Passwords.
- Remote access.
- Audit trails, including requiring officials to review change reports, such as a report of deletions or changes to data.
- Breach notification.

The Director told us that School officials were unaware of the need for these policies and generally relied on the IT service provider to handle all of the School’s IT related needs. Without these policies and procedures, the School has an increased risk that its hardware, software and data, including PPSI, may be exposed, damaged or lost through inappropriate access and use.

Also, without a policy requiring regular review of network and financial software audit trails and change reports, officials may not detect unauthorized or inappropriate activity within the network and financial software in a timely manner. In addition, if individuals’ private information is improperly accessed, officials may not be able to notify them in a timely manner. Furthermore, without an IT contingency plan, important financial and other data could be lost, or the School could suffer a disruption to operations, which could prevent the School from processing vendor payments and payroll checks.

How Should Officials Ensure Network and Financial Software User Account Access Controls Are Adequate?

School officials are responsible for restricting network and financial software user account access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure that data and IT assets on the network and in the financial software are secure from unauthorized use, modification and/or loss.

Network and financial software user accounts provide access to network resources and financial and employee data and should be actively managed to minimize the risk of unauthorized access and misuse. If not properly managed, unneeded user accounts may not be detected and disabled in a timely manner. Also, unneeded accounts are additional entry points for attackers. If compromised, these accounts could be used to potentially access and view PPSI, make unauthorized changes to accounting records or deny legitimate access to electronic information when needed.

To minimize the risk of unauthorized access, misuse and loss, officials should actively manage network and financial software user accounts and permissions, including their creation, use and dormancy. Officials should disable unneeded user accounts as soon as there is no longer a need for them, and regularly monitor them to ensure they are appropriate and authorized.

Officials should limit the use of service and shared accounts, routinely evaluate the need for them and disable those that are not related to a current school or system need. A service account is an account created for the sole purpose of running a particular network or system service or application (e.g., backups). Service accounts are not linked to individual users and, therefore, may have reduced accountability.

Shared user accounts are accounts with a username and password that are shared among two or more users. Shared accounts are often used to provide access to guests and other temporary or intermittent users (e.g., substitute teachers and third-party vendors). Because shared accounts are not assigned to an individual user, officials may have difficulty managing them and linking any suspicious activity to a specific user.

To help ensure individual accountability, each user should have and use their own user account, when possible. When shared user accounts are provided for temporary work or guests, the accounts should have an expiration date and automatically terminate access after a designated, authorized time period.

Generally, a network administrative account has permissions to monitor and control a network, connected computers and certain applications that can include adding new users and changing user passwords and permissions. A user with network administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, officials should limit network administrative permissions to those users who need them to complete their job duties and functions.

When financial software is used to process transactions and maintain financial records, school officials should establish adequate access controls that give users access to only those functions that are consistent with their job duties and responsibilities. Those involved in financial operations should not have access to user accounts with administrative permissions because an individual who has these permissions can generally add new users, configure software settings, override management controls, change user access rights and record and adjust financial transactions.

School officials should ensure that financial software access controls prevent users from being involved in multiple phases of financial transactions, or they should implement effective compensating controls, such as monitoring these users and the transactions that they process.

Officials should ensure that deletions and adjustments cannot be made without authorization and that there is a process in place for an independent party to review data entered into and changed in the software. These actions can help maintain the data's integrity.

Officials Did Not Adequately Control Network and Financial Software User Account Access

School officials did not adequately control network or financial software user account access. As a result, the School had unneeded user accounts, and accounts with unneeded user permissions, that were not disabled, removed or monitored.

We examined all 125 enabled School network user accounts (86 individual nonstudent accounts, 21 service accounts and 18 shared accounts)[1] and all three enabled financial software user accounts to determine whether the accounts and their permissions were needed and adequately controlled. As a result of our review and inquiry, 21 network user accounts (17 percent), including five with administrative permissions, were disabled or deleted, as follows:

Unneeded Individual Network User Accounts – We identified six individual network user accounts that had not been used in at least six months. After we asked School officials to review these accounts, they determined two were necessary and IT service provider staff (IT staff) disabled or deleted[2] four of the six accounts (67 percent) because they were no longer needed. These user accounts remained enabled much longer than necessary. The disabled and deleted accounts included:

[1] The School did not have any student network user accounts.

[2] While we typically recommend disabling accounts to preserve a clear audit trail, the IT service provider chose to delete certain accounts. When we discussed this with IT staff, they told us it was generally their practice to initially disable accounts and then delete them after three or more months.

- Two for vendor representatives who no longer worked at the School. We found that these user accounts had not been used in more than two years and four years, respectively.
- One for a former School employee. Although this employee left School employment in June 2020, the network user account remained enabled nearly two years later.
- One for an individual from an outside organization who never needed a School account. In addition, this account had unneeded administrative permissions.

These accounts should have been disabled as soon as the individuals left School employment or stopped providing services to the School. Generally, these accounts were still enabled because the School's written agreement with its IT service provider did not define expectations related to user account management.

Also, the School did not have adequate procedures for IT staff and School officials to follow to disable accounts. In addition, the IT service provider and School officials did not perform an effective periodic review of authorized users and their access to the network. While IT staff reviewed network user accounts, they did not identify the four unneeded user accounts.

Unneeded Service and Shared Network User Accounts – We found that 14 shared and 12 service network user accounts had not been used in the last six months. After we asked School officials to review these accounts, officials and the IT Manager told us that 12 shared and seven service network user accounts were unneeded.

Of these 19 user accounts, IT staff deleted or disabled 17 (10 shared and all seven service accounts) and allowed two shared user accounts to remain enabled. The IT Manager told us that he would delete the two remaining accounts in the future after further review. Five of these accounts, including one that remained enabled, had administrative permissions.

The Operations Manager and the IT Manager told us that the seven unneeded service accounts were for applications that the School no longer used, and the 10 shared accounts were previously used for various purposes, but were no longer needed. These user accounts remained enabled much longer than necessary. We found that two of these user accounts were not used in more than four years.

The IT Manager also said that the IT service provider performed an annual review of the School's network user accounts to identify any unneeded accounts. However, the IT Manager told us that this review did not include service or shared accounts or user permissions, including administrative permissions.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, possibly could be used to inappropriately access and view School data such as PPSI. When network user accounts are not monitored, compromised accounts may not be detected in a timely manner. In addition, when unneeded user accounts have administrative permissions, the School has an increased risk because the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

Unnecessary Financial Software Permissions – We identified two individual financial software user accounts and a shared account. The two individual user accounts were needed for authorized financial software users: the Operations Manager and the School's financial consultant.

We reviewed the financial software permissions for the two individual accounts to determine whether they were appropriate and adequately controlled. We found that both users' accounts had full access to all financial software modules, which included user permissions to change or delete transactions. Some of these permissions were not needed for these individuals' specific job duties and responsibilities.

In addition, the Operations Manager, assistant operations manager (who is involved in purchasing and other financial processes) and IT Manager unnecessarily shared access to the shared user account, which had administrative permissions. The Operations Manager told us that she and the assistant operations manager rarely used the shared account.

The Operations Manager told us they had access to the account to serve as the IT Manager's backup during his absence, if needed (the IT Manager was the financial software administrator). However, officials could have ensured that the IT Manager assigned another IT staff member to serve as his backup. When users share accounts, accountability is diminished and financial software activity may not be able to be traced back to a single user.

We examined the financial software and found that School officials did not ensure that access controls were adequate or establish compensating controls for the software control deficiencies. It also did not have necessary controls to maintain data integrity and deter inappropriate activity. The software allowed users to make changes to and delete transaction data – such as voiding transactions and deleting and adjusting data, including vendor names and disbursement amounts – without approval.

As a result, the School has an increased risk that unauthorized changes to the accounting records, software security settings and user authorization privileges could occur and go undetected. The risks associated with these inadequately controlled financial software permissions are increased because the Operations Manager signs School disbursement checks (under $5,000) using the Director's signature stamp without adequate oversight by the Director or another individual. When combined, these inadequate controls increase the risk of inappropriate School disbursements occurring and not being detected and corrected.

School officials did not establish adequate compensating controls for the software's deficiencies. For example, although audit trail and activity reports (such as a report of voided and deleted transactions) were available in the financial software, no one generated and reviewed them to determine who accessed the software and what activities they performed.

In addition, although officials performed an independent review of the School's bank statements, they did not review canceled check images because the images were not included with the bank statements. Therefore, no one reviewed the actual checks to determine whether they were written to the same vendors as recorded in the financial software.

We reviewed the sequence of recorded check numbers, the software's voided and deleted transactions report for entries that reduced cash and a sample of 55 check disbursements totaling $556,627.[3] We did not identify any questionable activity and found that all 55 check disbursements were for appropriate School purposes.

While we did not identify any questionable activity, allowing individuals the ability to alter, add and delete financial software data without oversight and approval increases the School's risk that inappropriate transactions could occur and remain undetected. For example, a user could conceal a theft by issuing an unauthorized check and then deleting the check or changing the vendor name in the financial software to conceal the inappropriate transaction. Because School officials did not review audit trail reports, including the voided and deleted transaction reports, School officials' ability to detect and properly address inappropriate activity was diminished.

Also, when School officials do not require each user to have and use a unique username and password and do not limit user permissions to only those needed for job duties, the School has an increased risk that unauthorized or inappropriate activity could occur within the financial software. Furthermore, when users share an account, accountability is diminished and questionable activity within the financial software may be difficult to trace to a specific user.

[3] Refer to Appendix B for further information on our sample selection.

How Does a Written Agreement With the IT Service Provider Help Ensure Network and Financial Software Access Controls Are Adequate?

To help adequately control a school's network and financial software access, and avoid potential misunderstandings, school officials should have a written agreement with the school's IT service provider. This agreement should establish the school's needs, clearly identify the IT service provider's roles and responsibilities and set the school's service expectations. The agreement also should include pricing, billing, payment terms and provisions for confidentiality to protect PPSI.

Furthermore, the agreement should be as specific as possible to establish comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. Agreements that are unwritten or lack these details can lead to indecision, disagreements or additional unanticipated costs. Officials should also periodically monitor the agreement to ensure compliance.

The School Did Not Have an Adequate Written Agreement with the School's IT Service Provider

School officials engaged an IT service provider to manage the School's IT operations, including support and services for network and financial software access controls. School officials had a written agreement with the IT service provider that contained provisions for pricing, billing, payment terms and protecting PPSI.

However, the agreement did not provide detailed information for the services to be provided, explain School and IT service provider responsibilities, or include comprehensive measurable performance targets. For example, the School's agreed upon compensation for all IT support and services for the 2021-22 school year was $90,922. But the agreement did not break down costs in detail to indicate the specific cost for each service, including those services directly related to network and financial software access controls.

Although the Operations Manager was responsible for overseeing the IT service provider, officials did not have procedures to monitor and review the work performed by the IT service provider. Therefore, officials could not ensure that the School's network and financial software data was adequately safeguarded.

Without an adequate written agreement and monitoring procedures, the School and IT service provider did not have stated responsibilities and procedures for network and financial software access controls. This can contribute to confusion over responsibilities for the various aspects of the School's network and financial software access control management, which could put the School's resources and data at greater risk for unauthorized access, misuse or loss.

Why Should School Officials Provide IT Security Awareness Training?

To help minimize the risk of unauthorized access to the network and financial software, and misuse or loss of data and PPSI, officials should provide periodic IT security awareness training that explains the risks inherent in – and proper user behavior needed when – accessing and using the network and financial software. In addition, the training should communicate related policies and procedures to all network and financial software users, including contractors.

The training could center on emerging cyberattack trends, such as information theft, social engineering attacks (methods used to deceive users into revealing confidential or sensitive information) and computer viruses and other types of malicious software. It could also explain how these trends and malicious software could result in the School's network, financial software and data being compromised, or users being denied access to them.

In addition, the training should cover key security concepts, such as the dangers of email, Internet browsing and downloading files and programs from the Internet; requirements related to protecting PPSI on the network or in the financial software; and how to respond if an information security or data breach is detected.

School Officials Did Not Provide IT Security Awareness Training

School officials did not ensure that network and financial software users received periodic IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets when accessing the network and financial software. The Director told us that they did not previously consider implementing IT security awareness training. However, this is a basic and fundamental security practice of which School officials or the School's IT service provider should have been aware.

Without periodic comprehensive IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of situations that could compromise the School's network and financial software. As a result, data and PPSI are at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Develop and adopt adequate written policies related to network and financial software access, including password, remote access and breach notification policies, and policies related to managing user accounts and reviewing network and financial software audit trails.

2. Develop and adopt a written IT contingency plan.

3. Ensure that the School's written agreement with its IT service provider includes the School's specific needs and expectations for IT services, roles and responsibilities of all parties, and comprehensive measurable performance targets.

The Operations Manager should ensure the IT service provider:

4. Disables unneeded network and financial software accounts or removes unneeded user permissions in a timely manner as directed by School officials.

5. Regularly generates user accounts and permissions reports for the network and financial software and submits the reports to School officials for review.

6. Eliminates shared user accounts for the network and financial software, or implements procedures to compensate for the inadequate user accountability of the shared accounts.

The Director should:

7. Sign checks or provide adequate oversight of her signature stamp.

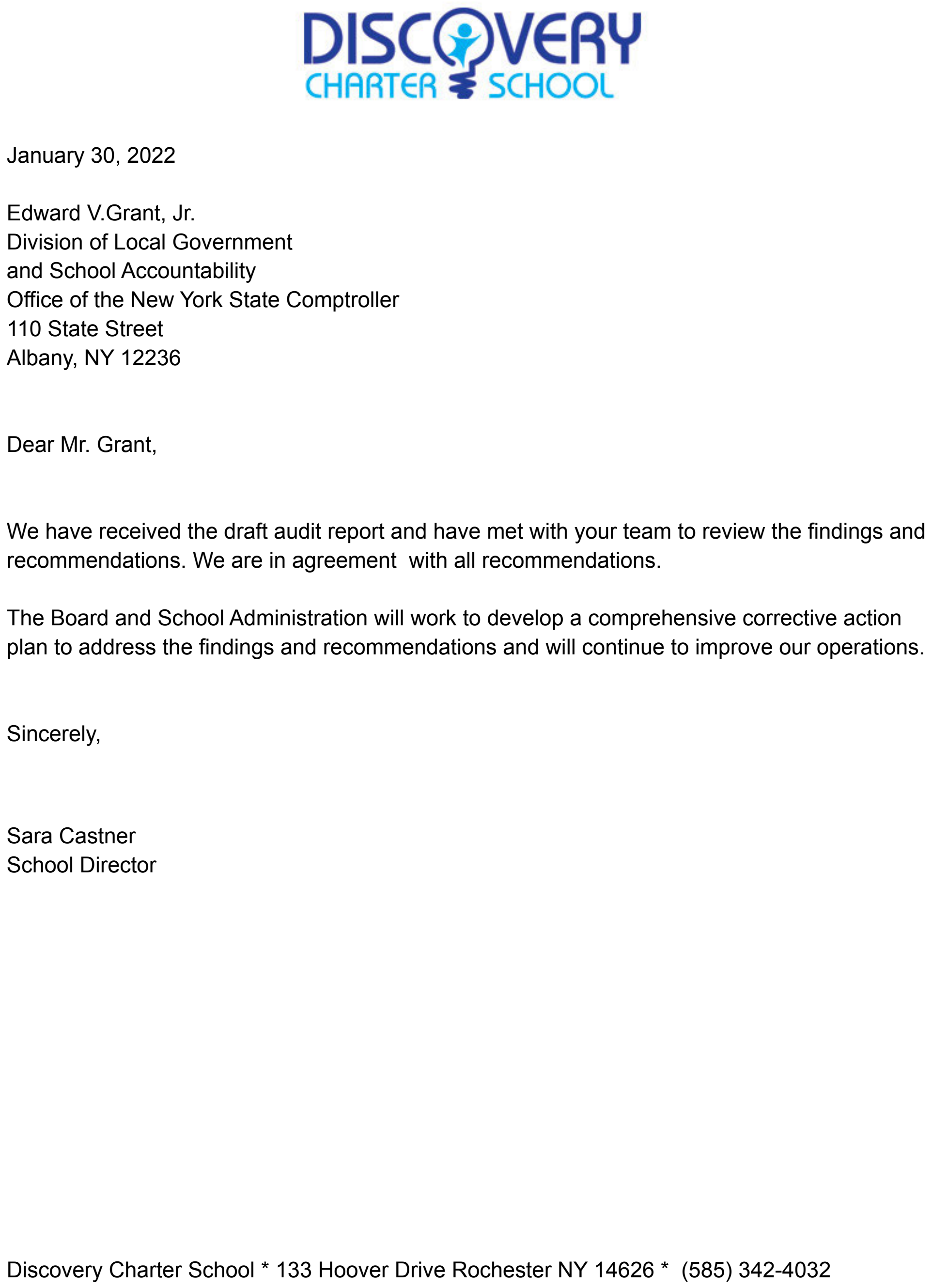
School officials should:

8. Designate a backup financial software administrator who is not involved in the School's financial operations.

9. Consider using alternative financial software or implement compensating controls for the software's deficiencies, such as an independent review of audit trail and change reports, canceled check images and check number sequences.

10. Provide periodic IT security awareness training to all network and financial software users.

Appendix A: Response From School Officials



January 30, 2022

Edward V.Grant, Jr.
Division of Local Government
and School Accountability
Office of the New York State Comptroller
110 State Street
Albany, NY 12236

Dear Mr. Grant,

We have received the draft audit report and have met with your team to review the findings and recommendations. We are in agreement with all recommendations.

The Board and School Administration will work to develop a comprehensive corrective action plan to address the findings and recommendations and will continue to improve our operations.

Sincerely,

Sara Castner
School Director

Discovery Charter School * 133 Hoover Drive Rochester NY 14626 * (585) 342-4032

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 in Section 2854 of the New York State Education Law, as amended by Chapter 56 of the Laws of 2014. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the School's IT and check disbursement policies and procedures and interviewed School officials and IT staff to gain an understanding of IT operations and controls, specifically those related to network and financial software access.
- We examined network user accounts and permissions using a computerized audit script, which we ran on March 30, 2022. We reviewed network user accounts and compared them to current employee lists to identify unused and possibly unneeded network user accounts and permissions. We discussed possibly unneeded network user accounts and permissions with School officials.
- We examined financial software user accounts and permissions as of March 10, 2022. We reviewed permissions for all three financial software user accounts to determine whether access was necessary and appropriate based on job duties and responsibilities.
- We reviewed recorded check number sequences and followed up on gaps in the numbering sequence, such as voids, because the financial software allowed changes and deletions to data.
- We assessed the adequacy of the School's written agreement with its IT service provider.
- We used our professional judgment to select 35 check disbursements (including all disbursements to business office staff and select disbursements for other School employees, the financial consultant and various vendors) and used a random number generator to select 20 check disbursements (55 disbursements) totaling $556,627. Our sample represented 10 percent of the 534 check disbursements totaling $3.3 million from July 1, 2020 through February 10, 2022. We chose this time period because it was the beginning of our audit period through the day after we held our entrance conference with School officials. We reviewed the supporting documentation (such as purchase order, purchase request forms and invoices) for the 55 disbursements to determine whether the disbursements were for a valid School purpose. We also compared the recorded disbursements to canceled check images.
- We reviewed all voided and deleted transactions (listed on a report generated from the financial software) that reduced cash during the period July 1, 2020 through May 5, 2022. We chose this time period because it was the beginning of our audit period through the date when we requested the

report. We compared the deleted transactions to general ledger activity to determine whether the deletions were reasonable (e.g., reversing duplicate entries). We reviewed supporting documentation for voided transactions to determine the reasons for the voids. We also reviewed bank statements to determine whether any voided or deleted checks cleared the bank.

Our audit also examined the adequacy of certain network and financial software access 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 plan of action that addresses the recommendations in this report and forward the plan 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.state.ny.us/files/local-government/pdf/regional-directory.pdf

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

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

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

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

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/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.state.ny.us/local-government/required-reporting

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

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

www.osc.state.ny.us/local-government

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties