DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-148

# True North Rochester Preparatory Charter School

## Information Technology

OCTOBER 2019

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

# Contents

# Report Highlights

## True North Rochester Preparatory Charter School

## Audit Objective

Determine whether the Board and School officials ensured information technology (IT) assets were safeguarded.

## Key Findings

- The Board did not adopt adequate IT policies or a disaster recovery plan.
- School officials did not provide IT security awareness training to staff.
- Hardware and software inventory records were inaccurate and outdated.

In addition, sensitive IT control weaknesses were communicated confidentially to School officials.

## Key Recommendations

- Adopt comprehensive IT policies and procedures and a disaster recovery plan.
- Provide security awareness training to staff and maintain complete and up-to-date hardware and software inventory records.

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

## Background

True North Rochester Preparatory Charter School (School) is located in the City of Rochester in Monroe County.

The School is governed by a Board of Trustees (Board) composed of nine members. The Board contracted with a charter management organization (Company) and delegated its authority for the management and implementation of both the academic and non-academic operations.

The School's IT network and assets are managed by an IT service provider who works closely with the IT Coordinator (Coordinator), an employee of the Company. The Coordinator is responsible for managing the day-to-day IT operations, while the IT service provider provides support for complex IT issues.

| Quick Facts | |
|---|---|
| **Enrollment** | 2,250 |
| **Employees** | 272 |
| **Number of Desktops, Laptops and Tablets** | 1,250 |

## Audit Period

July 1, 2016 – December 31, 2018

# Information Technology

The School relies on IT assets for Internet access, email and to maintain financial, personnel and student records.

## How Should the Board Safeguard IT Assets and Data?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board should establish security policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

School officials should have acceptable computer use policies that define allowable use and specific consequences for violations. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the school.[1]

Further, IT security policies should address data classification and regulations that ensure the protection of personal, private and sensitive information (PPSI),[2] password management, wireless security, online banking, user account management and permissions, sanitation and disposal of IT equipment, data backups, breach notification and disaster recovery. The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

## The Board Did Not Adopt and Officials Did Not Enforce Adequate IT Policies

<u>Acceptable Use Policies</u> – While the employee handbook contained a section offering limited guidance over computers, email and Internet use, the guidance was inadequate. The handbook guidance generally addressed Internet and email privacy and personal liability, but did not address personal use of IT assets or connecting personal devices to the network.

We reviewed the Internet browsing histories of 22 users on 22 computers[3] and found questionable and inappropriate Internet use on 16 computers. This included online shopping and gambling, visiting personal income tax preparation, entertainment, various fantasy sports and social media websites and website searches for jobs and real estate.

[1] Refer to our publication *Information Technology Governance* available at http://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

[2] Personal, private and sensitive information (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.

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

We also reviewed the 22 computers for specific file extensions and found more than incidental personal use on five computers. Four computers contained excessive amounts of personal photos[4] and one employee appeared to be using the School computer to bill the School for work performed by her father's personal business.[5]

Other IT Security Policies – The Board has not adopted IT security policies addressing data classification and regulations addressing the protection of PPSI.[6] Further, the Board has not adopted policies addressing password management, wireless security, remote access, online banking, user account management and permissions, sanitation and disposal of IT equipment, data backups, and breach notification.

In addition, School officials provided unrestricted remote access to two IT service providers: the IT provider responsible for managing day-to-day IT issues and the Company responsible for day-to-day business transactions. However, officials had no policies or procedures in place to monitor and review the work performed by these providers. Officials offered no explanation for not having these policies in place and told us that they relied on the expertise of their IT service provider to implement best IT practices.

While policies alone will not guarantee the safety of IT assets and data, a lack of appropriate policies significantly increases the risk that data, hardware and software may be lost or damaged by inappropriate use or access. Without formal policies that specify computer equipment use and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

## Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, school officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees and students. The training should center on emerging trends such as information theft, social engineering attacks[7] and computer viruses and other types of malicious software, all of which may result in PPSI compromise.

[4] Two of the four computers contained more than 2,500 photos that largely appeared to be personal.

[5] This employee had an invoice for a personal business open on her desktop and other files that contained the name of the business and mortgage documents at the time of our fieldwork.

[6] Such as practices to safeguard PPSI when collecting, storing, or transmitting information

[7] Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs. The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

## Employees Were Not Provided With IT Security Awareness Training

School officials did not provide users with IT security awareness training to help ensure they understand IT security measures. As a result, IT assets and data were more vulnerable to loss and misuse. For example, officials told us that employees connected personally-owned devices to School computers. Because teachers and other employees were not informed of the risks associated with connecting their own devices to School computers, these computers and the network could be compromised.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. School officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

## What Should Be Included in an IT Services Contract?

School officials must ensure that they have qualified IT personnel to manage the IT environment. This can be accomplished by using employees, an IT service provider or both.

To protect the School's IT assets and avoid potential misunderstandings, the School should have a written agreement with its IT service provider that clearly states the School's needs and expectations and specifies the level of service to be provided by the IT service provider. The agreement must include provisions relating to confidentiality and protection of PPSI and specify the level of service to be provided.

An IT agreement should establish comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It should provide detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology;

duration of the agreement; scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

## Officials Did Not Properly Contract for IT Services

The School relied on the Company[8] and an IT service provider[9] for managing its IT assets, and for IT services and technical assistance. School officials, used the same IT service provider the Company used for its IT support. However, officials did not have written contract with the service provider for the services provided.

Officials had a management agreement with the Company that governed the overall management of the School. It contained limited and vague language regarding the IT services the Company would provide. Specifically, the agreement called for the Company[10] to facilitate the School's purchase and procurement of IT equipment and services and provide certain computer and IT support for the School's programs, including troubleshooting, website and network design and completion of E-rate funding program applications.[11] However, the agreement did not contain sufficient information to clearly describe the rights and responsibilities of each party.

Because the School did not have a written contract with the IT service provider and instead relied on vague language contained in the management agreement, School officials were left with undefined roles and responsibilities for each party and had no guarantee of the type of services to be provided. Also, officials could not ensure that the Company or IT service provider had safeguards in place to protect the confidentiality of PPSI. Therefore, officials did not have any assurance that the School's IT system and data are properly safeguarded.

Without a written contract, the IT service provider did not have accountability for various aspects of the School's IT environment. As a result, the School had a greater risk that computer resources and PPSI could have been accessed by attackers, misused or lost.

[8] While the Company generally provided the day-to-day services necessary to operate the School, day-to-day IT services were managed by the IT Coordinator, an employee of the Company, who is based in New York City.

[9] The IT service provider was generally used for services needed by the School but not provided by the Company and was available on an as-needed basis.

[10] The agreement stipulated that the Company was responsible for the following: maintaining and providing training in the use of a central file server, providing training in the use of student information system, providing general desktop support to School staff and recommending and ensuring the effective implementation of a data backup protocol.

[11] The E-rate funding program allows eligible schools to receive discounts on telecommunications, telecommunications services and Internet access and internal connections, managed internal broadband services and basic maintenance of internal connections.

## Why Should the School Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, officials should establish a formal written disaster recovery plan (plan). This is particularly important given the current and growing threat of ransomware attacks.[12] The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the IT system, financial system and any PPSI contained therein.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

## The School Did Not Have a Disaster Recovery Plan

The Board did not develop a formal disaster recovery plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster or a phishing[13] or ransomware attack, staff had no guidance or plan to follow to restore or resume essential operations in a timely manner. Without a formal written plan, the School has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims.

## Why Should Officials Maintain Accurate and Up-to-Date IT Asset Inventory Records?

Computer hardware and software management is of particular importance to larger entities such as schools that have many different users who perform a variety of functions. Typically, schools have several software applications and multiple licenses[14] for each. Maintaining complete and comprehensive hardware

[12] Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made.

[13] Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.

[14] The purpose of a software license is to grant an end user permission to use one or more copies of a software program in accordance with the US Copyright Act, 17 US Code, Sections 101-810. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Schools must obtain licenses commensurate with the number of copies in use. The penalties for software licensing violations can be severe, exposing the school to legal liability, attorneys' fees and the expense of mandated IT audits.

and software inventory records is crucial in safeguarding IT assets from loss or theft, tracking the installation of unauthorized and unlicensed software on computers and avoiding fines for unlicensed software installations.

In addition, software installations or changes should be made by IT administration, or an IT service provider in the absence of an IT administration, to ensure that the software works well with the network and is for proper purposes. IT administrators also should ensure that the software is properly licensed. Officials should ensure that software inventory records include all school-owned software installed on computers and the number of copies and version currently in use.

The software inventory record should be used in conjunction with a comprehensive hardware inventory record, which details computer locations and users. These inventory records should be regularly reviewed and matched periodically with all school-owned computers to ensure that all IT assets are accounted for and installed software is properly approved and licensed. Maintaining complete and up-to-date hardware and software inventory records helps the board develop a formal IT asset replacement plan.

## IT Inventory Records Were Inaccurate and Outdated

Officials contracted with an IT service provider who maintained a hardware inventory list that included the device names and model and serial numbers, assigned users and locations, when applicable. During our review of account and security settings on 22 computers assigned to 22 users,[15] we found inconsistencies in the hardware inventory list. For example, one of the 22 users had a different computer than the one that was listed on the inventory and two other users and their computers were not listed on the inventory.

Because officials did not ensure that up-to-date hardware inventory records were maintained, they had an increased risk that IT assets could be lost, stolen or misused. Further, the Board's ability to develop a formalized IT asset replacement plan is hindered.

Additionally, officials did not maintain a comprehensive software and corresponding license inventory. Instead, the IT service provider maintained a list of approved software. However, the list did not include all the software downloaded on the 22 computers we reviewed, identify which computers contained the software or provide the number of installations of each version of software. We reviewed all of the software downloaded on 21 computers[16] and found 23 instances of software requiring licenses where School officials were unable to provide license documentation.

[15] See supra, footnote 3.

[16] Ibid.

Officials did not ensure that the IT service provider sufficiently monitored the software installed on School computers. Although the IT service provider told us that a software program he used had the ability to spot check computers for the software installed, this was only done on an as needed basis.

Without a complete and comprehensive software inventory, the School is at risk of violating its licensing agreements and allowing unauthorized software on School computers.

## What Do We Recommend?

The Board should:

1. Adopt acceptable use policies to include procedures for monitoring and enforcement, consequences for violating the policy and provisions for IT security awareness training.

2. Adopt comprehensive IT security policies to address password management, protection of PPSI, wireless technology, remote access, data classification, breach notification, sanitation and disposal of IT equipment, user account permissions and online banking.

3. Develop and adopt a comprehensive disaster recovery plan, including data backup procedures and offsite storage.

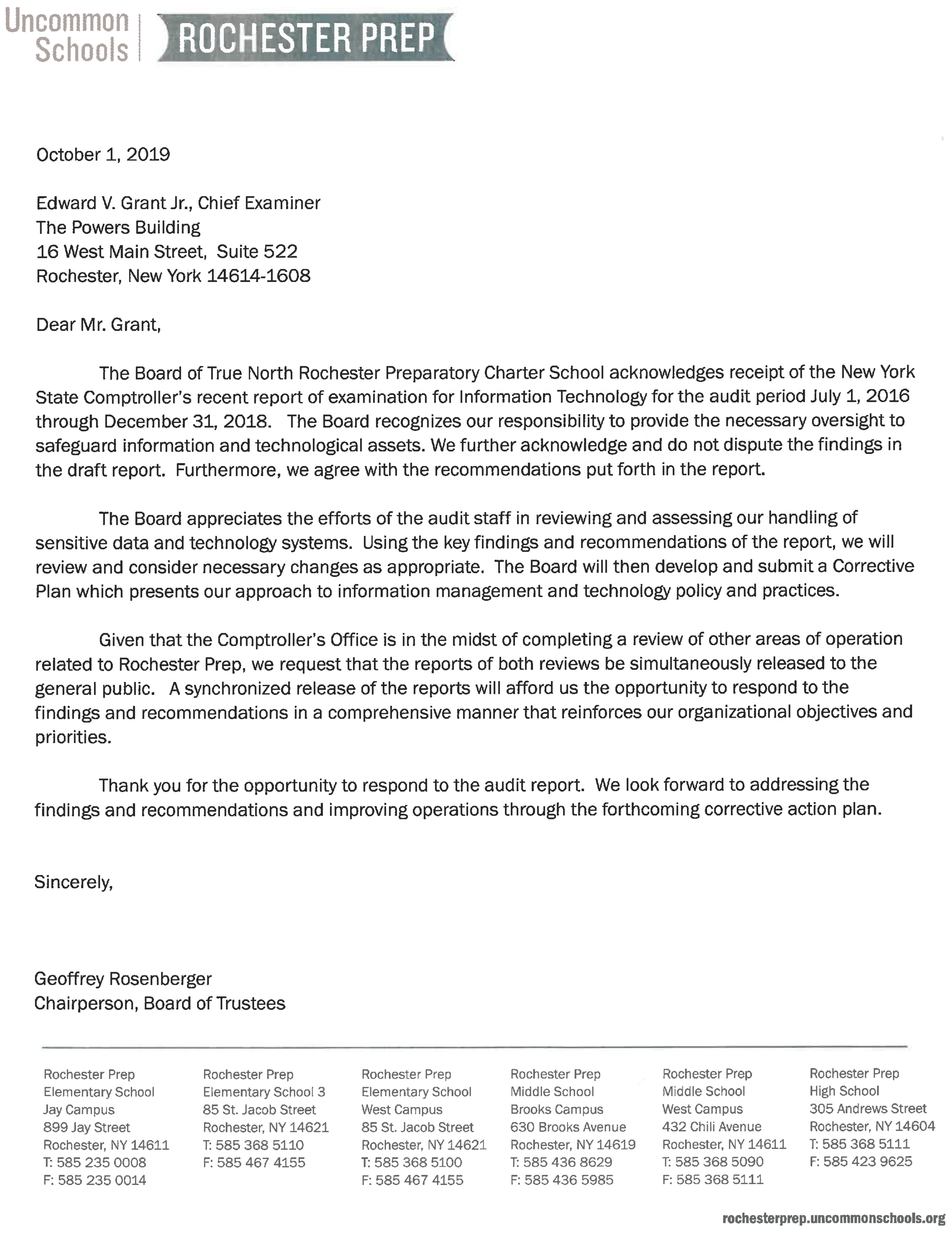
4. Enter into a professional service contract with the IT service provider that sufficiently defines the role and responsibilities of each party, includes all services to be provided and addresses confidentiality and protection of PPSI.

School officials should:

5. Provide periodic IT security awareness training to all staff who use IT resources that includes guidance on the importance of appropriate computer use.

6. Maintain accurate and up-to-date hardware and software inventories.

# Appendix A: Response From School Officials



Uncommon Schools | ROCHESTER PREP

October 1, 2019

Edward V. Grant Jr., Chief Examiner
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608

Dear Mr. Grant,

The Board of True North Rochester Preparatory Charter School acknowledges receipt of the New York State Comptroller's recent report of examination for Information Technology for the audit period July 1, 2016 through December 31, 2018. The Board recognizes our responsibility to provide the necessary oversight to safeguard information and technological assets. We further acknowledge and do not dispute the findings in the draft report. Furthermore, we agree with the recommendations put forth in the report.

The Board appreciates the efforts of the audit staff in reviewing and assessing our handling of sensitive data and technology systems. Using the key findings and recommendations of the report, we will review and consider necessary changes as appropriate. The Board will then develop and submit a Corrective Plan which presents our approach to information management and technology policy and practices.

Given that the Comptroller's Office is in the midst of completing a review of other areas of operation related to Rochester Prep, we request that the reports of both reviews be simultaneously released to the general public. A synchronized release of the reports will afford us the opportunity to respond to the findings and recommendations in a comprehensive manner that reinforces our organizational objectives and priorities.

Thank you for the opportunity to respond to the audit report. We look forward to addressing the findings and recommendations and improving operations through the forthcoming corrective action plan.

Sincerely,

Geoffrey Rosenberger
Chairperson, Board of Trustees

Rochester Prep
Elementary School
Jay Campus
899 Jay Street
Rochester, NY 14611
T: 585 235 0008
F: 585 235 0014

Rochester Prep
Elementary School 3
85 St. Jacob Street
Rochester, NY 14621
T: 585 368 5110
F: 585 467 4155

Rochester Prep
Elementary School
West Campus
85 St. Jacob Street
Rochester, NY 14621
T: 585 368 5100
F: 585 467 4155

Rochester Prep
Middle School
Brooks Campus
630 Brooks Avenue
Rochester, NY 14619
T: 585 436 8629
F: 585 436 5985

Rochester Prep
Middle School
West Campus
432 Chili Avenue
Rochester, NY 14611
T: 585 368 5090
F: 585 368 5111

Rochester Prep
High School
305 Andrews Street
Rochester, NY 14604
T: 585 368 5111
F: 585 423 9625

rochesterprep.uncommonschools.org

# 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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed IT policies in the employee handbook and interviewed School officials and the IT service provider to gain an understanding of IT operations and determine the adequacy of IT policies and procedures.
- Using the hardware inventory, the school organizational chart and conversations with School officials, we assigned a risk score to each of the users based on their access to the financial application, the student information system and whether they were in a managerial position. We categorized the users into various risk levels (very high risk, high risk, medium risk and low risk) based on the risk score. We used our professional judgment to select a sample size for each risk category and randomly selected 20 computers for the computer testing sample. In addition, we used the organizational chart to identify employees that did not appear on the hardware inventory and randomly selected three additional employees to add to our sample, which resulted in a testing sample of 23 computers. We identified 22 users who were assigned to these 23 computers. One user had two different computers listed on the hardware inventory. We chose to review only the computer that was actively used during our testing.

**Figure 1: Sample Composition**

| Risk Level | Total Number of Users | Percentage of Total Population | Computers in Our Sample | Percentage of Sample |
|---|---|---|---|---|
| **Very High** | 8 | 3% | 8 | 100% |
| **High** | 6 | 2% | 3 | 50% |
| **Medium** | 34 | 12% | 4 | 12% |
| **Low** | 242 | 83% | 5 | 2% |
| **Employee Not on Hardware Inventory** | | | 3 | 1% |
| **Total** | **290** | **100%** | **23** | **8%** |

- We used computerized audit software to obtain web histories, installed software and device settings for all 22 computers tested.[17] We reviewed specific security settings on 11 of these 22 computers that had administrative

[17] We were unable to obtain an installed software report for one computer because of a conflict with another installed program.

permissions and analyzed the results to determine whether they served a legitimate business purpose or presented any risk to the IT system.

- We compared serial numbers for our sample of computers tested to the School's IT hardware inventory.
- During our fieldwork, we walked through School facilities and observed physical security controls.

Our audit also examined the adequacy of certain information technology 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 GAGAS (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. 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 the relevant population size 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.

# Appendix C: Resources and Services

**Regional Office Directory**
www.osc.state.ny.us/localgov/regional_directory.pdf

**Cost-Saving Ideas** – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

**Fiscal Stress Monitoring** – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

**Local Government Management Guides** – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

**Planning and Budgeting Guides** – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

**Protecting Sensitive Data and Other Local Government Assets** – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/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/localgov/finreporting/index.htm

**Research Reports/Publications** – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

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

## 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/localgov/index.htm

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

**ROCHESTER REGIONAL OFFICE** – Edward V. Grant Jr., Chief Examiner

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, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller