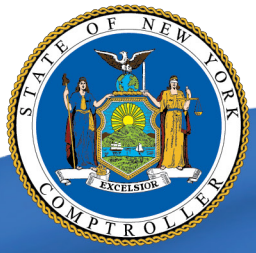
REPORT OF EXAMINATION | 2018M-172

Niagara Charter School

Information Technology

DECEMBER 2018



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

Contents

Report Highlights

Niagara Charter School

Audit Objective

Determine if personal, private and sensitive information (PPSI) on, or accessed by, the School's information technology (IT) assets is properly safeguarded, secured and accessed for appropriate School purposes.

Key Findings

- Personal computer and Internet use was found on seven computers.
- Virus scanning was either not activated or not up-to-date on three computers.
- PPSI was not classified and monitored to ensure protection from unauthorized access.

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

Key Recommendations

- Provide IT cybersecurity awareness training to employees who use IT assets and periodically monitor their use in accordance with the acceptable use policy.
- Ensure that virus protection is installed, activated and up-to-date on all computers.
- Classify PPSI to ensure its appropriate safeguarding.

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

Background

The Niagara Charter School (School) is located in the Town of Wheatfield, Niagara County. The School is governed by a Board of Trustees (Board) composed of five Trustees, two teacher trustees and two parent trustees. The Board is responsible for the general oversight of School operations. The Chief Academic Officer (CAO) is the School's chief executive officer and is responsible, along with other administrative staff, for the School's day-to-day management under the Board's direction. The School pays a contractor to serve as IT Coordinator, who oversees the School's IT environment and reports to the CAO.

Quick Facts	
2018 Budgeted Appropriations	$4.9 million
Employees	45
Students	350

Audit Period

July 1, 2017 – April 18, 2018

For certain audit tests, we expanded our audit scope back to June 15, 2015.

Information Technology

Schools rely on their IT assets to access the Internet and the cloud computing[1] environment for sending and receiving email messages and maintaining financial, personnel and student records and data. All of these activities may involve personal, private or sensitive information (PPSI).[2] Therefore, the IT systems and data (e.g., files, spreadsheets, system records) are valuable resources that need to be protected from unauthorized and inappropriate use. If IT systems or data are compromised, the results could range from inconvenient to severe and could require extensive effort and resources to evaluate and repair. A lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

What Is Effective IT Governance?

To provide effective governance of IT operations and minimize the risk of PPSI compromise, the governing board should establish computer policies that take into account people, processes, data and technology. Accordingly, school officials should develop and communicate written procedures for collecting, storing, classifying, accessing and disposing of PPSI encountered during the normal course of business. In addition, they should provide periodic cybersecurity awareness training that explains the proper rules of behavior for using the IT systems and data and appropriate Internet use, and communicate the school's policies and procedures to all employees.

Another key control to safeguard and secure PPSI is adequate virus protection. Virus definitions should be installed, activated and kept current. Officials should periodically monitor computers to ensure that virus protection is up-to-date and that virus scans are frequently performed.

School Employees Are Not Provided Cybersecurity Training

The IT security 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 the employees who use and/or manage IT understand the school's IT security policies and procedures and their roles and responsibilities related to IT and data security.

The School does not provide or require employees to attend any cybersecurity awareness training. Such training should center on emerging trends such as

1 Enables computer resources (such as files) to be stored and shared over the Internet.

2 PPSI is any information which – if subjected to unauthorized access, disclosure, modification, destruction or disruption of access or use – could severely affect critical functions, employees, customers, third parties or residents of New York State in general.

information theft, social engineering,[3] viruses and other types of malicious software, all of which may result in PPSI compromise. It 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; any requirements related to protecting PPSI; the risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected. Without cybersecurity awareness training, employees 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 are at greater risk for unauthorized access, misuse or loss.

We examined the School's documentation for all 10 in-house IT service calls from employees between March 2017 and January 2018 and identified seven that reported evidence of possible malware infections. Signs of infections might include slow, poor-performing computers. One January 2018 service call identified one computer containing 37 threats. While the IT Coordinator addressed these issues after they were brought to his attention, the overall risk of malware infections may be reduced with proper cybersecurity awareness training.

Some School Computers Were Used for Personal Activities

Internet browsing, especially of an inappropriate or personal nature, increases the likelihood of computers being exposed to malicious software that may compromise PPSI data. The School's acceptable use policy (AUP) states that laptops are issued for School business purposes and should not be used for personal email or web browsing. The AUP further indicates that the Internet is to be used primarily for business purposes and that computers may not be used for the purposes of compromising the School's information security system, transmitting sexually oriented information, gambling, hacking or purposes that violate any applicable law. The AUP establishes the School's right to monitor, review and audit each employee's computer and Internet use and, therefore, employees should expect no privacy when using the system.

While the AUP is contained within the School's employee manual and is annually reaffirmed and generally signed[4] by each employee, we identified personal Internet use on the majority of the computers we examined.

We judgmentally selected the computers of 11 of the School's 45 employees[5] for our testing to evaluate whether their Internet use was in accordance with

3 Social engineering is an attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information.

4 Signature indicates the employee has received and understands the School policies contained within the manual.

5 Our audit sample consisted of eight laptop and three desktop computers.

the AUP and whether the School properly monitored that use. We focused our testing on these employees due to their job title and general duties which indicated they were more likely than others to access the Internet and PPSI contained in financial or student records.

Our review identified personal Internet use on seven computers including activities such as online shopping, personal email, web searches for non-School related subjects such as job openings and real estate, and signing on to a non-School guest network.

The IT Coordinator and School officials were unaware of this personal computer use because they do not routinely monitor employee Internet usage for AUP compliance. As a result, IT assets and any PPSI they contain are at higher risk of undetected exposure to breach, loss, misuse or damage.

Current Virus Protection Is Not Activated On All Computers

The implementation and maintenance of adequate virus protection, including the routine updating of virus definitions, is critical for protecting PPSI residing on the School's IT system. Without current and up-to-date virus definitions, protection is limited and leaves computers at risk of being compromised by new types of emerging threats. Viruses can corrupt data and make computers inoperable, and can also lead to the disclosure of PPSI stored on, or accessed by, those computers. Damage caused by viruses can be expensive to fix and can cause significant losses in productivity until corrected. In addition to keeping virus definitions current, it is important to run virus scans on a routine and frequent basis.

While we found that virus protection was installed and available on all 11 computers in our sample, one computer did not have the installed virus protection activated and two computers had not been scanned for viruses in 30 and 44 days, respectively. These shortfalls were the result of inadequate oversight by the IT Coordinator, who told us he did not routinely monitor virus scan settings on all active computers.

PPSI Data Is Not Properly Classified

The School uses its IT system to collect and store data received and produced from its operations, including PPSI, which includes certain confidential financial, student and employee data. Classifying the PPSI data can help identify the type of security controls appropriate for its safeguarding.

School officials have not established a classification scheme for PPSI and, as a result, have not assigned a security level to that data. School officials do not know what PPSI has been retained, where it is located, who has accessed it

and whether it has been disposed of. As a result, School officials do not have adequate assurance that PPSI within the IT system is effectively and adequately protected from unauthorized access.

What Do We Recommend?

The Board should:

1. Ensure that periodic IT cybersecurity awareness training is provided to employees.
2. Ensure that employee AUP compliance is periodically monitored.
3. Adopt policies to address the classification and safeguarding of PPSI.

The Chief Academic Officer and IT Coordinator should:

4. Develop procedures to address the classification and safeguarding of PPSI.
5. Provide, or coordinate the provision of, periodic IT cybersecurity awareness training to all employees to address current and emerging trends and risks.
6. Conduct periodic reviews of employee computer and Internet use to ensure AUP compliance.
7. Ensure that virus protection is installed, activated and up-to-date on all computers, and that virus scans are routinely run.
8. Classify PPSI to ensure its appropriate safeguarding.

Appendix A: Response From School Officials

NIAGARA
Charter School

11/26/2018

Niagara Charter School
Information Technology
2018M-172-IT

To Whom It May Concern:

Please accept this correspondence as an Audit Response Letter and Corrective Action Plan (CAP) for Niagara Charter School in response to the findings of the 2018M-172-IT audit report and recommendations provided by your office.

Concerning the audit findings, Niagara Charter School agrees with the provided report and recommendations. For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed.

Audit Recommendation(s):

1. Provide IT cybersecurity awareness training to employees who use IT assets and periodically monitor their use in accordance with the acceptable use policy.
2. Ensure that virus protection is installed, activated, and up-to-date on all computers.
3. Classify PPSI to ensure its appropriate safeguarding.

Implementation Plan of Action(s):

1. Niagara Charter School is ensuring that periodic IT cybersecurity awareness training is provided to employees. After the conclusion of the audit, Niagara Charter School staff participated in cybersecurity awareness training provided by Erie1BOCES. Periodic cybersecurity training will be provided to all NCS staff to address current and emerging trends and risks. Training will be provided annually at the beginning of each school year, and subsequently throughout the school year as part of the school's professional development calendar.
2. Niagara Charter School is ensuring that virus protection is installed, activated, and up-to-date on all computers and that virus scans are routinely run. After the conclusion of the audit, the IT Coordinator used the findings proposed at the debrief meeting to manually configure each school computer with up-to-date, active virus protection. The IT Coordinator will create a monthly schedule to monitor the virus protection on each computer and device perpetually.
3. The Chief Academic Officer and IT Coordinator of Niagara Charter School will adopt policies to address the classification and safeguarding of PPSI. Reviews of employee computers and Internet use to ensure AUP (Acceptable Use Policy) compliance will be done periodically. PPSI will be classified to ensure its appropriate safeguarding on an annual basis. The periodic reviews of devices will be scheduled monthly to monitor usage and adherence to the AUP.

2077 Lockport Road Niagara Falls, NY 14304 PHONE: 716-297-4520 FAX: 716-297-4617
www.niagaracharter.org

NIAGARA
Charter School

Implementation Date(s):

1. Cybersecurity awareness training was provided to NCS staff by Erie1 BOCES on September 14, 2018. Beginning in January 2019, virtual professional development on cybersecurity awareness will be provided to staff from the IT Coordinator on a quarterly basis. NCS staff will be provided with cybersecurity awareness professional development and training annually, as well as throughout the school year.
2. After the conclusion of the audit, the IT Coordinator used the findings proposed at the debrief meeting to manually configure each school computer with up-to-date, active virus protection in July 2018. Beginning in January 2019, the IT Coordinator will create a monthly schedule to monitor the virus protection on each computer and device perpetually.
3. In May 2018, Niagara Charter School's CAO, IT Coordinator, and Board of Trustees initiated a policy manual review and update in coordination with Erie1 BOCES and the school's legal counsel. These policies include the Acceptable Use Policy (AUP) for school technology. Starting in January 2019, periodic reviews of devices will be scheduled monthly to monitor usage and adherence to the AUP.

Person Responsible for Implementation:

1. The CAO and IT Coordinator will ensure that periodic IT cybersecurity awareness training is provided to employees on an annual and on-going basis.
2. The CAO and IT Coordinator will ensure that virus protection is installed, activated, and up-to-date on all computers and that virus scans are routinely run.
3. The CAO, IT Coordinator, and the school's Board of Trustees will adopt policies to address the classification and safeguarding of PPSI in accordance with the school's AUP.

Niagara Charter School strives to provide our students and staff with a safe conducive learning environment. The findings and recommendations of the provided audit report will be used to enhance, foster, and improve the school's systems and operations. We thank you for providing Niagara Charter School with a thorough and comprehensive report.

Should you have any questions, concerns or feedback, please do not hesitate to contact me.

Sincerely,

Darci M. Novak
Chief Academic Officer

12/7/18
Date

2077 Lockport Road Niagara Falls, NY 14304 PHONE: 716-297-4520 FAX: 716-297-4617
www.niagaracharter.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 interviewed School officials and obtained and reviewed Board policies, meeting minutes and written procedures related to IT operations and PPSI safeguarding and classification.
- We interviewed School officials and viewed employee training logs to determine whether employees received IT cybersecurity awareness training.
- We examined the School's documentation for all in-house IT service calls to identify those submitted by employees between March 2017 and January 2018 and identified 10 such calls. We then assessed all 10 to determine whether any contained evidence of risk for malware infections. We judgmentally selected this time period to primarily coincide with the month the IT Coordinator started to maintain these records to the beginning of our audit to identify approximately a year's worth of activity. While service calls were also submitted by and for students during this time, we did not include those calls in this review because student user accounts were generally more restricted and had limited Internet access. However, due to the greater access to PPSI and the Internet and therefore greater risk of a PPSI compromise, we selected all employee-related service calls for this review.
- We provided a computerized audit script to the IT Coordinator to run on a judgmentally selected sample of 11 computers. We analyzed each report generated by the script, looking for potential issues including Internet browsing histories for personal and high-risk activities. Our sample selection was based on job titles that indicate duties likely to involve accessing student, staff and financial PPSI as follows: chief and assistant academic officers, business manager,[6] office manager, special education coordinator, counselor, nurse, cafeteria supervisor, administrative assistant and two teachers. We expanded our audit scope period back to June 15, 2015 because some of the employees' data extended back to that date.
- We observed virus security settings on each of the 11 computers in our sample to determine whether virus scanning was activated and, if so, how up-to-date the virus definitions were and when the last scan was performed.

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

6 The part-time business manager shares a computer with the office manager.

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 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.

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/lgli/pdf/cybersecurityguide.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

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

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