REPORT OF EXAMINATION | 2019M-9

Honeoye Central School District

Information Technology

AUGUST 2019

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

Contents

Report Highlights

Honeoye Central School District

Audit Objective

Determine whether the Board and District officials effectively managed the District's information technology (IT) assets.

Key Findings

- The Board and District officials have not adopted adequate security policies and procedures to safeguard IT assets.
- Employees stored personal data, such as photos, videos and music, on District computers.
- District officials did not provide IT security awareness training for employees.

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

Key Recommendations

- Adopt comprehensive IT security policies, procedures and plans to safeguard IT assets and data.
- Ensure staff comply with the District's policies related to personal use of IT assets.
- Provide periodic IT security awareness training to personnel who use IT resources.

District officials disagreed with certain aspects of our findings and recommendations, but indicated they have initiated corrective action. Appendix B includes our comments on issues raised in the District's response letter.

Background

The Honeoye Central School District (District) serves the Towns of Richmond, Bristol, Canadice, South Bristol and West Bloomfield in Ontario County and the Town of Livonia in Livingston County.

The Board of Education (Board) is responsible for managing the District's operations. The Superintendent of Schools (Superintendent) is responsible for the District's day-to-day management, budget development and administration.

The District contracts with Wayne Finger Lakes Board of Cooperative Educational Services (BOCES) along with another district for the shared services of an IT Director, network administrator and computer support specialist (BOCES IT staff) for the overall management of its IT infrastructure. At least one of these individuals is on-site daily.

Quick Facts	
Enrollment	568 students
Employees	227
Approx. # of Employee Computers	200
Computers Examined	13 Macs and seven PCs

Audit Period

July 1, 2017 – November 28, 2018

Information Technology

The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records. BOCES manages the District's Internet filtering, firewall and intrusion detection system.[1]

What Policies and Procedures Should the Board Adopt to Safeguard District 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 must 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.

District officials should have acceptable computer use policies that define allowable usage, specific consequences for violations and address IT security awareness training. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the district. The District's acceptable use policy prohibited the personal use of District computers, downloading Internet content onto District computers and connecting personal devices to the District's network.

Further, IT security policies should address data classification and regulations that ensure the protection of personal, private and sensitive information (PPSI),[2] breach notification, online banking, user access rights and sanitation and disposal of IT equipment. The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring policy compliance and the policies themselves.[3]

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

Acceptable use policies were not monitored or enforced.

Acceptable Use Policies – While the District had acceptable use policies for IT assets, they were not readily available for our review, disseminated to officials and staff, or enforced. In addition, the policies did not address connecting personal mobile computing and storage devices to the network, which can create security vulnerabilities and allow inappropriate access to IT assets and data.

1 A firewall is a software application or hardware device that filters traffic between a trusted network and an untrusted network, such as the Internet. An intrusion detection system (IDS) is a software application or hardware device installed on a network that detects and reports intrusion attempts. A firewall can block a suspicious connection while an IDS cannot.

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 For further information on these topics, refer to our publication *Information Technology Governance* at https://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

Because officials were unaware of the policies and their content, they could not monitor whether staff and students were appropriately using IT assets. Also, officials did not provide staff with required IT security awareness training to help ensure they understood IT security measures.

We reviewed the web browsing histories on the computers of 20 staff users[4] and found questionable Internet use for seven users, such as online shopping, use of personal email, visiting social networking, travel, news and entertainment websites, job searching and other websites that did not have a business purpose. We also reviewed the 20 computers for various file extensions and identified personal files, such as pictures, videos and MP3s on six computers. Two of the six computers had more than 2,000 pictures. In addition, during our review of seven of the 20 computers,[5] we found that two had personal fitness software installed and six had malicious software.

Because staff were not given a copy of the acceptable use policies or provided with IT security awareness training, they were unaware that they were violating the policy by visiting unacceptable websites, connecting personal devices to the District's network and putting the network at risk by downloading Internet content, which unintentionally included malicious software. BOCES IT staff told us they removed the malicious software from the computers we identified.

Other IT Security Policies – The Board did not adopt IT security policies addressing data classification, regulations to help ensure the protection of PPSI or a breach notification policy in the event that attackers access PPSI. It also did not adopt policies addressing online banking, user access rights or sanitation and disposal of IT equipment. During our audit fieldwork, the new IT Director prepared a plan for the Board to begin adopting missing and outdated IT policies.

Why Should the District Maintain Accurate and Up-To-Date Hardware and Software Inventory Records?

Computer hardware and software management is of particular importance to larger entities such as school districts that have many different users who perform a variety of functions. Typically, districts have several software applications and multiple licenses[6] for each. Maintaining complete and comprehensive hardware and software inventory records is crucial in safeguarding IT assets from loss

4 Refer to Appendix C for further information on our sample selection.

5 Ibid.

6 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.

or theft, tracking the installation of unauthorized and unlicensed software on computers and avoiding fines for unlicensed software installations.

IT administrators should ensure software is properly licensed. Also, officials should ensure that the software inventory record includes all district-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 checked and matched periodically with all district-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 also helps the board develop and implement an effective technology replacement plan.

Hardware and Software Inventory Records Were Not Comprehensive

The IT Director maintained a hardware inventory that included devices, model and serial numbers, assigned users, locations and inventory tag numbers, when applicable. However, the list was not comprehensive or updated. For example, during our review of the District's most current hardware inventory list, we found that the list did not include computers assigned to 26 employees.

Because officials did not maintain up-to-date hardware inventory records, the District had an increased risk that its IT assets could be lost, stolen or misused. Further, the Board's ability to develop an effective technology replacement plan was hindered.

District officials also did not maintain a comprehensive software inventory. The IT Director maintained an Excel spreadsheet that listed the names of software programs installed on District computers, but it did not identify specific licensing or version information. Also, the inventory did not indicate which computers were using licensed software.

Officials told us that BOCES was responsible for seeking procurement of software and tracking pertinent licensing information. BOCES IT staff told us they intended to track the software currently installed on all District computers and update the software and hardware inventory during the summer of 2019. Because officials did not maintain a comprehensive software inventory list, the District is at risk of violating its licensing agreements and allowing unauthorized software on District computers.

Why Should Officials Monitor User Accounts?

User accounts enable the system to recognize specific users and provide access to networks and computers. To minimize the risk of unauthorized use, officials should develop comprehensive procedures for actively managing these accounts, including their creation, use and dormancy. When user accounts are no longer needed, officials should ensure that these accounts are disabled in a timely manner.

Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if necessary.

The District Had Unneeded User Accounts

The District did not implement comprehensive procedures for monitoring user accounts. During our review of the District's 833 enabled network user accounts for staff and students, we found that 332 accounts (40 percent) had not been used in the last six months.

The majority of these accounts (317) were student accounts. Students used Chromebooks[7] that did not require authentication to the District's network, which accounted for the length of time that these accounts went unused. We also found that the District had 46 generic network user accounts and 10 of these accounts had not been used in the last six months.

Because the District's network had unused, unneeded active network user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to compromise IT resources. In addition, by allowing employees to use generic accounts, officials could not have identified single users who may have performed unauthorized activities.

BOCES IT staff told us they intended to review all user accounts during the summer of 2019 and update them accordingly.

7 Chromebooks are laptop computers that run the Google Chrome operating system. They are used primarily while connected to the Internet.

What Do We Recommend?

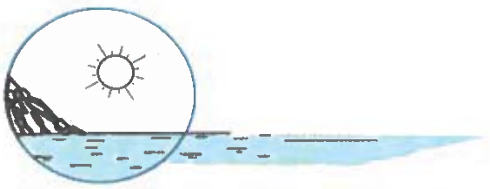
The Board should:

1. Provide a copy of all acceptable use policies for IT assets to officials, staff and students.
2. Update the acceptable use policies to address connecting personal mobile computing and storage devices to the District's network. Also, periodically review and update all IT policies and procedures to reflect changes in technology and the District's computing environment.
3. Adopt comprehensive IT security policies addressing data classification, regulations to help ensure the protection of PPSI, breach notification, online banking, user access rights and sanitation and disposal of IT equipment.

The IT Director should:

4. Develop procedures for monitoring Internet usage and inactive user accounts and enforcing the acceptable use policies.
5. Limit the ability of District staff to download and install inappropriate software and personal files on District computers.
6. Provide periodic IT security awareness training to all personnel who use IT resources, which includes the importance of appropriate computer use and safe web browsing practices.
7. Ensure the hardware inventory list is updated and comprehensive.
8. Ensure the software inventory list is updated and comprehensive and includes specific licensing and version information and a description of the computers that the software is installed on and those using licensed software.
9. Develop comprehensive procedures for monitoring user accounts and disable those accounts that are no longer needed.

Appendix A: Response From District Officials



Honeoye Central School
8528 Main Street
Post Office Box 170
Honeoye, New York 14471-0170
585-229-4125
Fax # 585-229-5633
Web Page: Honeoye.org

David C. Bills, Superintendent

July 1, 2019

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 Examiner Grant:

Thank you for your thorough and thoughtful report regarding the State of New York Comptroller's Audit of the Honeoye Central Schools Technology Department.

We are responding today at your request, addressing your preliminary draft findings found in the Report of Examination dated June 24th, 2019 and the subsequent exit meeting, where we discussed items that we feel may be inaccurate or incomplete. Because we have not received the updates made to the Report of Examination document at the time of or after the meeting, our response today will follow the original document from beginning to end, noting various points of interest.

Items of note:

1. *Background Section* - Please note that a new IT administrator started in the district as the audit began.
2. *Background Section* - Please note in the third paragraph that the whole site based IT department is comprised of part-time BOCES employees totaling 1.3 FTE.
3. *Background Section* - The enrollment number for Honeoye Central Schools as of Sept 13, 2018 should be 568.
4. *Pg 4 - Policies and Procedures* - The second paragraph inaccurately states that personal devices are connected to the district's network. The district only provides basic internet access to personal devices through our wireless infrastructure.
5. *Pg 4 - Enforcing Adequate IT Security Policies* - The second paragraph should note that students use, almost across the board, use Chromebooks. These devices are managed and the district receives alerts when inappropriate access is attempted. Additionally, students sign an appropriate use policy as a part of their Student Handbook.
6. *Pg 5 and 6 - Up-to-Date Hardware and Software Inventory Records and the Comprehensive section.* There is a need to clearly state the current understanding of what defines software. The majority of software used now is either Cloud based or completely web based. This concept is referenced in the Report of Examination and seems to reduce the significance of some of the specifics you require for software inventories, as the cloud based systems do not allow you to extend past your

See Note 1 Page 9
See Note 2 Page 9
See Note 3 Page 9

Honeoye Central School
8528 Main Street
Post Office Box 170
Honeoye, New York 14471-0170
585-229-4125
Fax # 585-229-5633
Web Page: Honeoye.org

David C. Bills, Superintendent

purchased license count, and are often times tied to specific users inside of the software package's administrative console. Some packages that now do this include but aren't limited to: Adobe, Microsoft, Google Chromebook licenses, GoGuardian licenses, Mobile Device Manager licenses, etc. These are our primary software packages. Additionally, there are times where we must install software purchased privately by a teacher (personal printer, camera, clipart, equation editors, etc).

See Note 4 Page 9

7. *Pg 6 - Monitor User Accounts and Unneeded User Accounts* - The district does need to maintain their Active Directory accounts for a variety of reasons including: single sign-on applications, student information system access, and a number of other ancillary software packages. However, most students do not need to utilize their active directory accounts directly during their academic, as they log into Google on their Chromebooks, which do not authenticate to the domain.
8. *Pg 6 - Monitor User Accounts and Unneeded User Accounts* – Teachers and/or anyone who uses a Mac computer on a daily basis does not currently authenticate to the domain.
9. *Pg 6 - Monitor User Accounts and Unneeded User Accounts* - Please include a note that the auditors were made aware that the district's Smart Schools Bond Act submission does include monies to be spent to upgrade the network infrastructure that would make authentication possible from Macs and Windows machines.

The items relayed in this letter were composed by our current IT Director, Dr. Ryan Arthurton and our BOCES IT support team. They have worked diligently during this process to start making corrective actions to many of the items that were shared in your report, prior to the report being published. We look forward to finalizing our official corrective action plan in the weeks ahead.

Sincerely,

David Bills
Superintendent of Schools
Honeoye Central Schools

Cc:
Keith Stumbo, President Honeoye Board of Education
Ryan T. Arthurton, IT Director

Appendix B: OSC Comments on the District's Response

Note 1

The report was updated to include this information.

Note 2

Personal mobile computing and storage devices were connected to the District's network by staff using their District-provided computers. This was also confirmed by the IT Director during our exit conference.

Note 3

The report was updated to include this information.

Note 4

District officials should maintain a complete and accurate inventory list to ensure software is appropriate, compatible and in compliance with all applicable laws and regulations regardless of whether it is installed locally or web-based.

Appendix C: 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 Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- Using permissions and access reports provided by District officials, we ranked (highest to lowest risk) all 203 staff IT users based on their level of access and permissions to various IT programs and equipment. From this ranking, we used our professional judgment to review 20 users by choosing the top seven PC users who had the highest level of access and permissions to IT programs and equipment and by randomly selecting 13 other Mac users who also had the highest level of access and permissions. District employees used a mixture of PCs and Macs.[8]
- We manually reviewed the hard drives of all 20 selected computers to determine whether they contained installed or downloaded files that were inappropriate or did not serve a business purpose.
- We used specialized audit software to examine the web browsing histories of the seven PCs and manually examined the web-browser histories of the 13 Macs.
- We used specialized audit software to examine installed software on the seven PCs and manually reviewed installed software on the 13 Macs.
- We used specialized audit software to examine local account (individual computer) and network security settings on the seven PCs.
- We used specialized audit software to review all enabled accounts on the District's network.
- We reviewed hardware and software inventory lists to determine whether they were accurate and comprehensive.
- During our fieldwork, we walked through the District's 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 District 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

8 Mac computers run on the Mac OS (operating system) and are made only by Apple Inc. PCs (personal computers) run on the Windows operating system, produced by Microsoft Corp., and are made by many manufacturers, such as HP (Hewlett-Packard), Acer Inc., Lenovo PC International and Dell Inc.

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.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-1(3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the fiscal year. 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. We encourage the Board to make the CAP available for public review in the District Clerk's office.

Appendix D: 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