REPORT OF EXAMINATION | 2018M-141

Finn Academy: An Elmira Charter School

Information Technology

NOVEMBER 2018

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

Contents

Report Highlights

Finn Academy: An Elmira Charter School

Audit Objective

Determine whether Board and School officials effectively managed information technology (IT) assets.

Key Findings

- The Board did not develop adequate IT policies and procedures.
- School officials did not provide IT security awareness training to employees.
- The Board did not develop a disaster recovery plan.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt written IT policies and procedures.
- Provide periodic IT security awareness training to personnel who use IT resources, including the importance of physical security and protection of personal, private, sensitive information (PPSI).
- Develop a disaster recovery plan.
- Address the IT recommendations communicated confidentially.

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

Background

The Finn Academy: An Elmira Charter School (School), located in the City of Elmira, is governed by a Board of Trustees (Board) composed of six members. School officials contract with a certified public accounting firm for overall financial management and bookkeeping services. The Board appoints a Chief Operations Officer (COO), who is responsible, for the day-to-day management under the Board's direction.

School officials contract with three service providers for IT support.

Quick Facts	
Grades Served	Kindergarten – Grade 5
IT Users	385
Employees	47

Audit Period

July 1, 2016 – June 26, 2018

Information Technology

The School relies on its IT assets for Internet access, email, financial recordkeeping, online banking and to maintain confidential PPSI. If IT assets are compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of assets and data, 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.

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. Therefore, it is essential for the board to establish IT security policies for all IT assets and information. The school should have acceptable computer use policies that define the procedures for computer, Internet and email use and include IT security awareness training requirements for staff.

Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the school.[1] 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 Adequate IT Security Policies and School Officials Did Not Enforce

While acceptable use is briefly and vaguely discussed in the School's employee handbook and confidentiality policy, it is not adequate, monitored or enforced. Specifically, officials do not describe the expectations concerning personal use of IT equipment, address connecting and using personal IT equipment for valid purposes or define the consequences of policy violations. Connecting personal devices to the School's network can create security vulnerabilities and allow inappropriate access to School IT assets and data. Further, the policies do not require cybersecurity training.[2]

We reviewed users' web browsing histories on 14 computers[3] and found questionable Internet use for nine users, such as online shopping; use of personal email; visiting social networking, travel, news and entertainment websites; job

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

2 Refer to "Why Should Officials Provide IT Security Awareness Training?" section of report.

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

searching; and other personal websites (e.g., Pennsylvania child abuse history clearances, free application for federal student aid, student loans, Zillow and Turbo Tax).

The Board has not adopted IT security policies addressing password management, breach notification, protection of PPSI, wireless technology, mobile devices, remote access, sanitation and disposal of IT equipment, user accounts, online banking and data backups. Without formal policies that explicitly convey the appropriate 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?

Computer users must be aware of security risks and trained in practices that reduce internal and external threats to IT systems and data. While IT policies tell computer users what to do, IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on:

- Emerging trends in information theft and other social engineering reminders;
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet;
- Password controls;
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed;
- Restricting physical access to IT systems and resources; and
- Protecting IT systems from intentional or unintentional harm, loss or compromise.

Officials Did Not Ensure IT Security Awareness Training Was Provided

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 are more vulnerable to loss and misuse. For example, during our review of IT assets, we found that staff usernames and passwords were written on sticky notes attached to their computing devices or in their classrooms.

Why Should the School Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may

include any sudden, catastrophic event[4] that compromises the availability or integrity of an IT system and data. 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. 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 they will function as expected.

The Board Did Not Adopt a Disaster Recovery Plan

The Board did not adopt a disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, School officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data.

Without a disaster recovery plan, the School could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process grades and State aid claims.

What Should Be Included in IT Service Provider's Contracts?

The board must ensure that they have qualified IT personnel to manage the school's IT environment. This can be accomplished through employees, an IT service provider or both. To avoid potential misunderstandings and to protect IT assets, the school should have a written agreement with the provider that clearly states the school's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI and specify the level of service to be provided.

The Board Adopted Inadequate IT Service Provider Contracts

The School relies upon two private IT service providers for network hosting, IT services and technical assistance and the Greater Southern Tier Board of Cooperative Educational Services (BOCES) for internet filtering and firewall/ intrusion detection services. We found that the contracts with the private providers were inadequate because needs and expectations were not clearly stated and the contracts did not address confidentiality or PPSI. Furthermore, the BOCES contract did not specifically discuss firewall parameters and how intrusions will be monitored.

4 Such as a fire, computer virus or inadvertent employee action

Insufficient, nonexistent or vague agreements can contribute to confusion over who is responsible for various aspects of the IT environment, which puts data and computer resources at greater risk for unauthorized access, misuse or loss.

Why Should Officials Maintain IT Software Inventory Records?

Software management is of particular importance to schools that have many different users who perform a variety of functions. Typically, schools have several software applications and multiple licenses[5] for each. The implementation of a complete and comprehensive software inventory list is crucial to safeguard IT assets from the installation of potential unauthorized and unlicensed software.

As a best practice, the list should include all school-owned software installed on computers and the number of copies currently in use. Additionally, the list should be used in conjunction with a comprehensive hardware inventory list that details computer locations and users and regular reviews of all school-owned computers, to ensure that all software installed is properly approved and licensed. Software additions or changes should be made by IT administration, when practical, to ensure that the software works well with the network, is safe to use and is for school use.

School Officials Did Not Maintain IT Software Inventory Records

School officials did not maintain a software inventory, even though the COO told us that there is little software used. Without a complete and comprehensive software inventory, officials have no assurance that all installed software is appropriately licensed and for valid purposes. Furthermore, it is unlikely that software patches necessary to address known vulnerabilities will be applied on a timely basis, if at all. Our review of 14 School computers found outdated and unnecessary software on the School's computers.

What Are Strong Access Controls?

School officials are responsible for restricting users' access to those applications, resources and data that are necessary for their day-to-day learning, duties and responsibilities to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. User accounts enable the

5 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, additional attorneys' fees and the expense of mandated IT audits.

system to recognize specific users, grant the appropriately authorized access rights and provide user accountability by affiliating user accounts with specific users, not sharing user accounts among multiple users and disabling generic user accounts.

Users with administrative rights and remote access must also be limited and all access should be monitored. Finally, all users should set their own passwords within prescribed requirements. Holding passwords to certain complexity, length and age requirements makes passwords more difficult to crack or be easily guessed.

Officials Did Not Implement Strong Access Controls

School officials did not implement comprehensive procedures for managing, limiting, securing and monitoring user access. As a result, we noted inactive user accounts and inadequate password requirements. For example, 14 of the 385 users (4 percent) have not been used in the last six months and three of the accounts (1 percent) do not match current employees. Consequently, the IT assets and data are at increased risk for loss or misuse.

What Do We Recommend?

The Board should:

1. Update the acceptable use policies to limit connecting personal IT equipment, describe the expectations concerning personal use of IT equipment, include provisions for IT security awareness training and define the consequences of policy violations.

2. Adopt comprehensive IT security policies addressing password management, breach notification, protection of PPSI, wireless technology, mobile devices, remote access, sanitation and disposal of IT equipment, user accounts, online banking and data backups.

3. Periodically review and update all IT policies and procedures to reflect changes in technology and the computing environment and stipulate who is responsible for monitoring all IT policies.

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

5. Enter into contracts with the IT service providers that sufficiently define the role and responsibilities of each party, includes all services to be provided and address confidentiality and protection of PPSI.

School Officials should:

6. Develop procedures for monitoring internet usage and enforcing the acceptable use policies.
7. Provide periodic IT security awareness training to personnel who use IT resources, including the importance of physical security and protection of PPSI.
8. Maintain an up-to-date software inventory.
9. Develop comprehensive procedures for managing, limiting, securing and monitoring user access.

Appendix A: Response From School Officials

Finn Academy:
An Elmira Charter School
610 Lake Street, Elmira, NY 14901

607.737.8040
info@finnacademy.com
www.finnacademy.com

October 12, 2018

Edward V. Grant Jr.
Chief Examiner
Division of Local Government and School Accountability
State of New York Office of the State Comptroller
The Powers Building
16 West Main Street
Suite 522
Rochester, NY 14614-1608

Dear Mr. Grant,

As indicated in your letter of September 14, 2018, we are submitting our formal response to you concerning the preliminary draft findings of your recent examination of Finn Academy: An Elmira Charter School. We have addressed each of the draft audit report findings and recommendations in the chart below:

Audit Finding	Finn Academy Response
The Board Did Not Adopt Adequate IT Security Policies and School Officials Did Not Enforce	Since the publication of the audit we have updated and distributed our new Employee Manual, which contains an updated Acceptable Use Policy for all employees that specifically addresses various concerns listed in the audit report. In terms of web browsing history, we maintain that many of the websites visited are not for personal use but are visited in support of the unique curriculum we deliver, i.e. visiting a recipe website is mentioned which would be connected to school use in the creation of our Finn Summer Session Wellness Cooking Challenge Cookbook. Various procedures listed in the audit report, i.e. password management, breach notification, wireless technology, mobile devices, etc. are indeed in place, but are not formally adopted policies of the Finn Academy Board of Trustees.

See Note 1 Page 11

Finn Academy:
An Elmira Charter School
610 Lake Street, Elmira, NY 14901
607.737.8040
info@finnacademy.com
www.finnacademy.com

	These procedures are being documented in writing and will be reviewed by the Governance Committee of the Board of Trustees and put forth for approval by Finn's full Board of Trustees.
Officials Did Not Ensure IT Security Awareness Training Was Provided	An IT Security Awareness Training program was implemented beginning on October 3, 2018. All staff members participated in training highlighting concerns addressed in the audit. Ongoing IT Security Awareness will be conducted in partnership with our IT partner, [redacted]
The Board Did Not Adopt a Disaster Recovery Plan	Finn Academy does have a Disaster Recovery plan in place, it is just not formally documented and approved; this will be addressed at the Committee level and moved up to the full Board of Trustees at an upcoming meeting for adoption.
The Board Adopted Inadequate IT Service Provider Contracts	Finn Academy had service provider contracts in place with all providers; we will work with our service providers to implement contracts containing more in-depth information that will be more acceptable to the standards set forth by the Office of the State Comptroller.
School Officials Did Not Maintain Software Inventory Records	At the time of audit, a software inventory list did not exist, however, installed software was regular reviewed by [redacted] Our IT consultants will continue to periodically download a report of all software that is installed on user devices and it will be reviewed by the COO; local admin rights have been prohibited for all users; an inventory system has been put in to place to document and approve when new software is added to a user's device.

See Note 2 Page 11

See Note 3 Page 11

Finn Academy:
An Elmira Charter School
610 Lake Street, Elmira, NY 14901
607.737.8040
info@finnacademy.com
www.finnacademy.com

Officials Did Not Implement Strong Access Controls	We have internally audited the access controls and ensured the access controls are in place and implemented on each user's device; again, procedures were in place, just not documented and formally approved by the Board of Trustees.

See Note 4 Page 11

Please be advised that we will write and adopt a Corrective Action Plan, as required, and submit that to your office prior to the 90-day deadline.

If you have questions or require further information, please contact me at 607.737.8040 or martinabaker@finnacademy.com.

Sincerely,

Martina Baker
Chief Operations Officer

Appendix B: OSC Comments on the School Officials' Response

Note 1

Questionable Internet use was discussed with School officials and no business purpose was identified at that time for staff visiting sites related to personal email, social networking, travel, news and entertainment, job searches, and other personal websites, such as those for income tax preparation. We removed recipe websites from the list of personal websites visited in our report.

Note 2

During audit fieldwork, School officials and the IT consultants told us that a disaster recovery plan did not exist, which we confirmed with them at the pre-exit and exit conferences. In addition, because a software inventory was not maintained, officials are unaware about what data is maintained by staff or how to recover lost data in the event of a disaster.

Note 3

At the beginning of our audit fieldwork the IT consultants told us that School employees and officials had administrative rights to add software without any oversight, which we confirmed with our review of 14 computers. Although School officials told us that the IT consultants regularly reviewed installed software, our review of 14 computers identified outdated and unnecessary software, which were confidentially communicated.

Note 4

Had access control procedures been in place and working effectively, we could not have identified 14 users that had not been active in the last six months or three accounts that were not for current employees.

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:

- We reviewed Board minutes and adopted IT policies and procedures and interviewed School officials and IT service provider representatives to gain an understanding of the IT operations and determine whether the IT policies and procedures were adequate.
- We examined the network account and security settings using specialized audit software. We reviewed the user and administrator accounts and compared them to current employee lists to identify inactive and unnecessary accounts. We reviewed automated settings and compared them to best practices.
- We judgmentally selected seven users based on their positions[6] and randomly selected eight users from the other employees (from a user list provided to us by an IT service provider). One randomly selected user was no longer employed by the School, therefore we tested 14 computers in total.
- We used specialized audit software to obtain web histories, installed software, patch levels and device settings for our previously selected sample. We analyzed the results to determine whether employees engaged in inappropriate or questionable Internet activity, PPSI was exposed in web addresses, webpages or public documents, these computers were currently or previously infected with malicious software, users downloaded or used potentially unwanted programs and installed software served legitimate purposes or presented any risk to the IT system.
- We reviewed the IT service provider contracts to determine whether they clearly stated the needs and service expectations, contained provisions relating to confidentiality and protection of PPSI and the level of service to be provided.
- We walked throughout the facilities and documented our observations of physical security controls.

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

We conducted this performance audit in accordance with GAGAS (generally accepted government auditing standards). Those standards require that we

6 The COO, school nurse, coordinator of special education and interventions, registrar, administrative assistant, dean of academics and dean of scholars

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 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 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/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

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