REPORT OF EXAMINATION | 2018M-61

King Center Charter School

Information Technology

JULY 2018

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

Contents

Report Highlights

King Center Charter School

Audit Objective

Determine whether information technology (IT) assets are properly safeguarded, secured and accessed for appropriate School purposes.

Key Findings

- The Board has not adopted adequate IT security policies and School officials do not have formal procedures to address breach notification, disaster recovery, data backup, password security management, IT asset inventory and user access rights.
- We identified inappropriate or questionable computer use on six computers.

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

Key Recommendations

- Adopt written IT policies and procedures to address breach notification, disaster recovery, backups, password security management, IT asset inventory and to address individual user access rights.
- Provide IT cybersecurity awareness training to personnel who use the School's IT resources.

In addition, we confidentially communicated key IT recommendations to School officials.

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

Background

The King Center Charter School (School) is located in the City of Buffalo. The School is governed by a Board of Trustees (Board) composed of 11 Trustees and three parent representatives. The Board is responsible for the general oversight of School operations. The Principal 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 IT Director is responsible for day-to-day IT operations and reports to the Director of Finance and Operations (Director).

Quick Facts	
2017-18 Budgeted Appropriations	$5.9 million
Employees	78
Students	450

Audit Period

July 1, 2016 – December 8, 2017

For certain audit tests, we expanded our testing back to May 4, 2013.

Information Technology

The School relies on its IT system for Internet access, email, and maintaining and accessing personal, private or sensitive information (PPSI)[1] including financial, personnel and student records. Therefore, the IT systems and data are valuable School resources. If IT systems are compromised, the results could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of an IT system, 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 Information Technology Governance?

To provide effective governance of IT operations and minimize the risk of a PPSI compromise:

- The Board should:
  - Establish computer policies that take into account people, processes and technology; communicate the policies throughout the School; and ensure School officials develop procedures to monitor compliance with policies.
  - Ensure the IT Director maintains detailed, up-to-date inventory records for all computer hardware and software. The information maintained for each item should include a description including the make, model and serial number and the employee (or student) name to whom the item is assigned.
- School officials should:
  - Develop and communicate written procedures to grant, change and terminate access rights to networked computer systems and specific software applications. Passwords should be held to certain requirements to make passwords more difficult to crack or be guessed. Criteria could include complexity requirements, length, aging, reuse of old passwords and also address failed log-on attempts.
  - Develop and provide periodic IT cybersecurity awareness training that explains the proper rules of behavior for using the School's IT systems and data and communicate the School's policies and procedures that need to be followed.

1 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.

The Board and School Officials Have Not Established Sufficient IT Policies and Procedures

The Board has not adopted a policy for notifying students and staff, in the event there is a PPSI compromise or breach. Further, the Board has not adopted a comprehensive disaster recovery plan to describe how officials will respond to potential disasters, which could include sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that compromise the network and financial system availability or integrity and any PPSI contained therein. Typically, a disaster recovery plan involves the analysis of business processes and continuity needs, a focus on disaster prevention, the roles of key individuals and the precautions necessary to maintain or quickly resume operations.

Also, the Board did not adopt a policy and officials did not develop written procedures to provide guidance on data backups that define the frequency and scope of backups, the location of stored back-up data and the specific method for backing up data (e.g., encryption). Even though the IT Director backs up data at regular intervals, he does not verify that the data has been properly backed up and can be restored.

Further, the Board did not require and the IT Director did not routinely provide periodic report updates to the Board addressing actual and potential issues affecting the School's IT assets, such as IT inventory updates, current trends in cybersecurity awareness and resources needed and applied to maintain the School's IT system.

Without established policies and formal written procedures addressing notification of a breach of PPSI, disaster recovery, data backups and periodic reporting to the Board, there is an increased risk that the School could lose important financial data and suffer serious interruption in operations.

The School's Technology Plan Does Not Establish Safeguards for IT Assets

The Board adopted a long-term technology plan (Plan) which outlines an evaluation process, including the establishment of a technology plan committee (Committee) that is responsible for formally evaluating the Plan twice each year. However, the Board has not established the Committee. Instead, the Plan is periodically reviewed by the Director and the IT Director and included in the School's charter renewal. Additionally, while the Plan addresses how students will use IT for educational purposes, the Plan does not indicate how IT assets will be physically safeguarded from theft or misuse. Staff and students annually receive a reminder of acceptable use policies for IT assets. However, without appropriate oversight and monitoring, the risk of inappropriate computer use is increased which could compromise the IT system data, including PPSI.

The School Does Not Have a Complete or Reliable Inventory List

The Board has not adopted a policy and officials have not developed written procedures for maintaining an IT asset inventory. Although the IT Director provided us an inventory list that he maintained, it was not accurate or complete.

During our IT asset physical examination, we found two projectors and 18 wireless access points[2] in use that were not on the IT Director's inventory list. Further, we selected 13 of 50 computers listed on the inventory that were assigned to employees and found three which did not have serial numbers listed on the inventory list. As a result, the IT Director could not demonstrate with certainty that those three computers were in fact properly assigned to the respective employees. Moreover, while each employee generally signs a "loan of equipment" form (form) when the IT Director assigns a computer, we found that one computer was not the same computer for which the employee had signed and subsequently presented to us for our review. The IT Director could not account for the computer that the employee indicated was received on the form.

Additionally, in 2014, the School reported 88 laptops as stolen. However, we found that the serial numbers of 18 of the reported stolen laptops were still included on the IT inventory list. Of these 18, we included nine in our inventory testing and found that seven were currently being used by the School. Due to the inaccurate and incomplete inventory list, the current IT Director and officials were not aware that this was the case.

The Board and School officials cannot properly protect IT assets and operations if they do not know what IT resources they have. Because neither the previous nor the current IT Director maintained a detailed, up-to-date inventory record, the School remains at an increased risk of loss.

The School Has Insufficient Access Controls

The Board has not adopted a policy and School officials have not developed comprehensive written procedures for establishing, modifying or deleting user accounts or appropriate controls over passwords (e.g., complexity requirements, password age). The IT Director is responsible for establishing user accounts and authorizing network access. Without adopted policies and procedures for monitoring and revoking user access rights, officials did not have an effective process in place to notify the IT Director of changes to employees' employment status. Inactive user accounts increase the risk for attacks on the School's networks.

2 A wireless access point is a networking hardware device that allows a Wi-Fi device to connect to a wired network.

We found that the network had 16 inactive user accounts that have not been used in over six months, six of which were never used. In addition, five of the accounts were unnecessary and five were for students that are no longer enrolled at the School. Unnecessary network user accounts should be disabled or removed as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete PPSI. Of particular risk are user accounts for former employees, as these could potentially be used by those individuals for malicious activities. Further, unnecessary accounts create additional work to manage access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

Computer Scans Indicate Inappropriate or Questionable Internet Use

Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise PPSI. The School's acceptable use policy states that it prohibits the use of computers for non-educational or illegal purposes, while the School's Internet use policy specifically prohibits using School resources for gambling.

We examined web history and Internet use on six computers for a total of four teachers, the IT Director and the Director and determined that all six engaged in inappropriate and/or questionable Internet use such as: online shopping, travel planning, social networking and gambling websites.

Teachers are allowed to take their assigned computers home throughout the year, including over the summer when classes are not in session.[3] When computers are not connected to the network, they do not have the security controls in place, such as firewall protection, and therefore are at a greater risk of virus, hacking or a breach.

The School's acceptable use policy is part of the employee handbook that each employee signs when they are hired. Our scans identified two user profiles that had indications of malicious software and potentially unwanted programs. However, the IT Director and other officials were unaware of this because they do not monitor employee Internet use or firewall activity. In addition, the School does not provide cybersecurity training to staff. Not providing cybersecurity training to employees increases the risk that users will not understand their responsibilities, putting the School's data and IT assets at greater risk for unauthorized access, misuse or abuse. As a result, IT assets and any PPSI contained therein are at higher risk of exposure to breach, loss, misuse or damage.

3 School officials indicated this allows teachers to plan and prepare work for their upcoming classes.

What Do We Recommend?

The Board should:

1. Adopt written IT policies to address breach notification, user access rights, disaster recovery, data backups, password security management and IT asset inventories.

2. Periodically review and update all IT policies to reflect changes in technology and the School's computing environment.

3. Establish the Committee in accordance with the Board's long-term technology Plan and update the Plan to address how IT assets will be physically safeguarded from theft or misuse.

4. Ensure School officials develop and provide IT cybersecurity awareness training at least annually to personnel who use the School's IT resources.

The IT Director and School officials should:

5. Develop detailed written procedures that supplement adopted IT policies.

6. Provide periodic reports to the Board so that it can provide sufficient oversight of IT operations such as, potential and actual issues affecting IT assets and PPSI contained therein, updates made to the IT system and inventory adjustments.

7. Update and maintain a reliable and complete inventory of IT assets.

8. Follow-up on the IT inventory issues noted in this report and determine whether the original report of 88 stolen laptops is accurate and whether there are any additional unaccounted-for laptops that should be reported to the proper authorities.

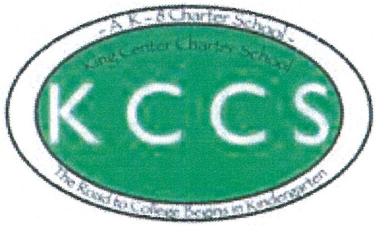
9. Evaluate all existing network user accounts, disable or remove any deemed unnecessary and periodically review user accounts for necessity and appropriateness.

10. Provide adequate oversight of Internet use and firewall activity to ensure use is in accordance with Board policies.

11. Evaluate the security of IT assets that are removed from School premises (e.g., laptops taken home for the summer) and ensure sufficient security measures are in place.

12. Prepare and annually provide IT cybersecurity awareness training to personnel who use School IT resources.

Appendix A: Response From School Officials



156 Newburgh Avenue, Buffalo, NY 14211

July 11, 2018

Mr. Jeffrey D. Mazula
Chief Examiner of Local Government and School Accountability
State of New York Office of the State Comptroller
Buffalo Regional Office
295 Main Street, Suite 1032
Buffalo, NY 14203

Dear Mr. Mazula:

The Board of Trustees has reviewed your draft audit report of King Center Charter School's Information Technology for the period of July 1, 2016 – December 8, 2017. We welcome your expertise and feedback on how to strengthen our internal controls.

We understand the need to continually revisit and evaluate the effectiveness of our internal controls on an on-going basis, especially the potential damages because of a security breach. We also appreciate the opportunity to have had an exit conference on June 19, 2018 to further discuss the findings and clarify specific items noted in the audit.

Based on the audit recommendations the following corrective actions have been taken or proposed. The Board is committed to developing a corrective action plan within 90 days of the date of the preliminary report. Following is our actions already taken or proposed:

- The Board should adopt written IT policies and procedures to address breach notification, user access rights, disaster recovery, data backups, password security management and IT inventories.
- The IT Director has followed-up on the IT inventory issues noted in the audit report to determine the accuracy of the original figures.
- The IT Director and School Officials will prepare and annually deliver IT cybersecurity awareness training to all personnel using School IT resources.
- The IT Director and School Officials have updated and will maintain a reliable and complete inventory of IT assets.
- The IT Director and School Officials will provide oversight of Internet use and firewall activity to ensure use is within Board policies.

The Board of Trustees for King Center Charter School accepts the recommendations as written in the report.

Sincerely,

Michelle A. Martin

Interim President – Board of Trustees

Cc: Antoinette Rhodes, Principal
Carl Morgan, Co-Treasurer – Board of Trustees
Scott Saperston, Co-Treasurer-Board of Trustees
Barbara Lindaman, Director of Finance and Operations

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 obtained and reviewed Board policies and minutes, School procedures related to IT operations and assets and interviewed School officials to obtain an understanding of the IT environment.
- We interviewed the IT Director regarding the School's procedures for maintaining an IT inventory and then obtained the current IT inventory report and compared it to recent IT purchases and physical inventory to determine whether it was accurate and complete.
- We interviewed the Director regarding any police reports or insurance claims the School has filed reporting any stolen or missing IT assets. We then obtained from the Director the 2014 police report and insurance claim filed reporting 88 stolen laptop computers. We compared this information with the current IT inventory list to determine whether the IT inventory list was updated accordingly. We noted that the serial numbers for 18 of these 88 laptops were still on the IT inventory. As such, we judgmentally selected half (50 percent) of the 18 laptops and nine laptops that were previously reported as stolen and sought to locate them while performing a physical IT inventory.
- We interviewed School officials about the process followed, including whether there were any written guidelines or procedures, for granting access to the School's network, reviewing specific access and permissions granted to individual users and removing and modifying permissions in a timely manner.
- We provided an audit script to the IT Director on a universal serial bus driver to run on a judgmentally selected sample of six laptop computers. We analyzed each report generated by the script, looking for potential issues including Internet browsing histories for personal and high-risk activities. Our judgmental sample selection was based on employee job titles and length of employment with the School. Our sample of laptop computers included four teachers who have been employed by the School for over two years and two administrative staff.
- We obtained a list of all School network users and compared it to current payroll reports and student enrollment reports to determine whether any users were not currently employed or enrolled with the School.
- We interviewed School officials to determine whether employees received cybersecurity awareness training or reviewed acceptable use policies regularly.

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 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