



Pittsford Central School District

Security of Personal, Private and Sensitive Information (PPSI) on Mobile Computing Devices and Extracurricular Cash Records and Collections

Report of Examination

Period Covered:

July 1, 2014 – January 21, 2016

2016M-92



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	1
EXECUTIVE SUMMARY	2
INTRODUCTION	4
Background	4
Objectives	4
Scope and Methodology	5
Comments of District Officials and Corrective Action	5
PPSI ON MOBILE COMPUTING DEVICES	6
Security Policies and Procedures	6
PPSI Testing	7
PPSI Data Classification and Inventory	8
Recommendations	8
EXTRACURRICULAR CASH RECORDS AND COLLECTIONS	10
Extra-Classroom Collection Records	10
Extra-Classroom Receipts	11
Extracurricular Deposits	12
Athletic Event Admissions	12
Recommendations	13
APPENDIX A Response From District Officials	15
APPENDIX B OSC Comment on the District's Response	23
APPENDIX C Audit Methodology and Standards	24
APPENDIX D How to Obtain Additional Copies of the Report	25
APPENDIX E Local Regional Office Listing	26

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

August 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Pittsford Central School District, entitled Security of Personal, Private and Sensitive Information (PPSI) on Mobile Computing Devices and Extracurricular Cash Records and Collections. This audit was conducted 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.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller
Division of Local Government
and School Accountability*



State of New York Office of the State Comptroller

EXECUTIVE SUMMARY

The Pittsford Central School District (District) is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction. District officials are responsible for developing comprehensive written policies and procedures to properly protect personal, private and sensitive information (PPSI)¹ from unauthorized access on the District's nearly 3,050 mobile computing devices (MCDs). The Board and District officials are also responsible for protecting and overseeing the District's extracurricular cash assets, including extra-classroom activity fund money and athletic event admission fee collections.

Scope and Objectives

The objectives of our audit were to determine if the District adequately safeguarded PPSI on MCDs and extracurricular cash collections for the period July 1, 2014 through January 21, 2016. Our audit addressed the following related questions:

- Have District officials adequately safeguarded MCDs to prevent unauthorized access to PPSI?
- Have District officials provided adequate oversight of cash collections for extra-classroom activity funds and athletic events?

Audit Results

District officials need to improve their security policies and procedures to ensure District MCDs are adequately safeguarded and prevent unauthorized access to PPSI. Our review of 80 District-owned MCDs disclosed PPSI on 16 (20 percent) of these devices. Without proper safeguards in place, any confidential data on these MCDs could be at risk of exposure. We also found that District officials have not developed a classification scheme or performed an adequate inventory of the PPSI stored on District MCDs. Unless District officials identify all the PPSI maintained, it could be difficult to

¹ PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general. Private information could include one or more of the following: Social Security number, driver's license number or non-driver identification card number, account number, credit card number, debit card number and security code, or access code/password that permits access to an individual's financial account or protected student records. See <https://www.its.ny.gov>.

promptly notify the affected students and their families and other parties if a data security breach should occur.

In addition, District officials need to improve their oversight of cash collections for extra-classroom activity funds and athletic events. Officials did not implement policies and procedures over athletic event admissions and adopt procedures to ensure adequate reconciliations of extracurricular cash collection activities were prepared. District officials did not ensure that sufficient documentation was maintained for cash collections and prenumbered cash receipts were issued for all money collected.

We identified 29 cash receipts totaling \$17,577 (15 extra-classroom activity receipts totaling \$12,327 and 14 athletic event fees totaling \$5,250) that were not deposited within the three-day period allowed by District policy. These funds were deposited from four to 15 days after they were received. In addition, the athletic director did not monitor or periodically reconcile the athletic event ticket inventory to account for the number of tickets sold. As a result of these discrepancies, District officials were unable to determine if all ticket money collected was deposited. When adequate records are not maintained and periodically reconciled, there is an increased risk that fraud and concealment could occur and remain undetected.

Comments of District Officials

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

Introduction

Background

The Pittsford Central School District (District) is located in the Towns of Pittsford, Brighton, Mendon, Penfield and Perinton in Monroe County and the Town of Victor in Ontario County. The District is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District operates nine schools with approximately 5,700 students and 1,200 employees. The District's budgeted appropriations for the 2015-16 fiscal year were \$122.6 million, which were funded primarily with State aid, sales tax and real property taxes and grants.

The District has a centralized Information Technology (IT) department headed by a chief information officer. The Director of Technology is responsible for directing the day-to-day operations of the IT department and staff, which includes overseeing the purchase of computer hardware, software and supplies and the security of the central information systems and network. The department also oversees and maintains all of the District's approximately 3,050 MCDs, which are distributed to administrators, teachers and students. The types of mobile computing devices (MCDs) used at the District include laptop and tablet computers, smart phones and digital music players.

The Board and District officials are responsible for protecting and overseeing the District's extracurricular cash assets, including extra-classroom activity fund money and fees collected for admission to athletic events. During 2014-15, the District's 96 extra-classroom activity fund accounts recorded receipts totaling \$631,980 and disbursements totaling \$650,093 and had a combined cash balance of \$233,187 as of June 30, 2015. In addition, the District deposited \$10,871 from athletic event admissions.

Objectives

The objectives of our audit were to determine if District officials adequately safeguarded personal, private and sensitive information (PPSI) on MCDs and cash collections for extracurricular activities for the period July 1, 2014 through January 21, 2016. Our audit addressed the following related questions:

- Have District officials adequately safeguarded MCDs to prevent unauthorized access to PPSI?

- Have District officials provided adequate oversight of cash collections for extra-classroom activity funds and athletic events?

Scope and Methodology

We examined the safeguarding of PPSI on MCDs and extra-classroom and athletic event admission cash collections for the period January 1, 2014 through January 21, 2016. 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 District officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix C of this report. 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.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education, 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, with a copy forwarded to the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next 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. The Board should make the CAP available for public review in the District Clerk's office.

PPSI on Mobile Computing Devices

District officials are responsible for developing comprehensive written policies and procedures to properly protect PPSI² from unauthorized access, clearly communicating these policies to staff and monitoring compliance. While computer policies will not guarantee the safety of a computer system, a lack of appropriate policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. It is also important that District officials are aware of the different kinds of data they possess so they can make informed decisions about setting appropriate security levels. To do this, officials should conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data maintained.

District officials need to improve their security policies and procedures to ensure District MCDs are adequately safeguarded and prevent unauthorized access to PPSI. Our review of 80 District-owned MCDs disclosed PPSI on 16 (20 percent) of these devices. Without proper safeguards in place, any confidential data on these devices could be at risk of exposure. We also found that District officials have not developed a classification process or performed an adequate inventory of the PPSI stored on the District MCDs. Unless officials identify all the PPSI maintained, it could be difficult to promptly notify the affected students and their families and other parties if a data security breach should occur.

Security Policies and Procedures

Effective policies and procedures for protecting PPSI address various aspects of securing the data and limiting access to it. Policies should be clearly communicated and define the devices covered (e.g., organizationally owned or personally owned), procedures for reporting lost or stolen MCDs and storage devices, the process used for gaining approval before connecting new devices to the system and user responsibilities. The District should also address how PPSI should be stored, if necessary for business purposes, and the ramifications for not following District procedures. District officials should classify information in a consistent manner to determine the

² PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general. Private information could include one or more of the following: Social Security number; driver's license number or non-driver identification card number; account number, credit card number, debit card number and security code, or access code/password that permits access to an individual's financial account or protected student records. See <https://www.its.ny.gov>.

level of security each type of data needs and conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data maintained.

The District provides laptop and tablet computers and smart phones for staff use and allows staff to connect personally owned MCDs to the District's network resources for email services. While the District has an email policy which includes a statement advising staff not to transmit PPSI, the District does not have an acceptable use policy governing the connection of personally owned MCDs to its network resources. The District's website provides directions for staff to connect these devices to its email services. However, there are no established security procedures in place governing this practice.

District officials have not adopted policies and procedures for staff use of personal removable storage devices (e.g., flash drives) or addressed security features such as passwords or data encryption, if PPSI is allowed on these devices. The District does not provide removable storage devices for staff use, so any use would be on personal devices. As a result, District officials have no assurance that PPSI is not transferred from the secure District network to these devices or that such information is properly secured.

District officials have also not adopted procedures to follow, in the event personally owned MCDs are lost or stolen, that require staff who connect their devices to District email resources to notify District officials. While the email service allows officials to remotely erase data from lost devices, this practice was not communicated to those staff connecting personal devices to the District's network. The loss or theft of these devices could cause inappropriate and costly exposure of PPSI that the District is responsible for safeguarding. The failure to properly ensure that all devices connected to the District's network resources are secure increases the risk that PPSI could intentionally or accidentally fall into the wrong hands.

PPSI Testing

While there may at times be a legitimate business need for PPSI to reside on these devices, it is the responsibility of District officials to determine who should have access to sensitive information and whether or not an MCD is the best medium on which to store such information. If such a determination is made, District officials are responsible for ensuring that adequate safeguards are in place on MCDs to prevent unauthorized access to this information.

We tested for the presence of PPSI on District-owned MCDs used by staff during our audit period. We examined 80 such MCDs, which included laptop and tablet computers, smart phones and digital music players. We found that 16 (20 percent) of these devices contained

PPSI, such as personal student information, credit card information and account usernames. The exposure of PPSI to any unauthorized users would constitute a data security breach, which could have negative financial consequences for the individual(s) whose private information was accessed. Such exposure could also have a negative financial impact on the District as custodian of this data, if it were found liable for the unauthorized release of confidential information. The occurrence of data security breaches also reduces residents' confidence in the District's ability to safeguard personal information about students and their families.

PPSI Data Classification and Inventory

All information, whether in printed or electronic form, should be classified and labeled in a consistent manner to ensure data confidentiality, integrity and availability. The data classification process assigns a level of risk to various types of information, which helps management make appropriate decisions about the level of security the data requires.³ District officials should also conduct an inventory of PPSI stored on all types of electronic equipment used to ensure the data classification process is comprehensive. In the event of a data breach, the proper classification and inventorying of PPSI allows District officials to determine the extent of unauthorized access and take appropriate action.

District officials had an inventory list of data elements prepared, which included the types of information used by the District's various software applications. However, officials did not have a PPSI inventory prepared evaluating where the data resides (i.e., physical location), such as the specific device or server. In addition, PPSI has not been inventoried or classified based on risk to account for the confidential data maintained. As a result, District officials are unaware of the extent to which PPSI resides on the electronic equipment used by District staff and students on a daily basis. Unless District officials classify the data they maintain and set appropriate security levels for PPSI, there is an increased risk that PPSI could be exposed to unauthorized users and efforts to properly notify affected parties in the event of a data breach will be hampered.

Recommendations

District officials should:

1. Adopt formal written policies and procedures to ensure a sound IT environment and protect PPSI on MCDs. These policies and procedures should outline the proper access, use and protection of PPSI on MCDs and address personally owned devices connecting to District network resources.

³ An example of a data classification scheme can be found in the OSC guide, *Information Technology Governance*, available at <http://www.osc.state.ny.us/localgov/pubs/lmgm/itgovernance.pdf>

2. Ensure that a complete classification and inventory of PPSI stored on all District computer equipment is prepared to ensure data confidentiality, integrity and availability. The classification and inventory list should be updated on an ongoing basis, as appropriate, to reflect any changes.

Extracurricular Cash Records and Collections

The Regulations of the Commissioner of Education (Regulations) require each school district's board of education to adopt rules and regulations to safeguard, account for and audit all money received and derived from extra-classroom activities. The Regulations provide procedures for extracurricular activities that charge admission fees and cash collections. The Board and District officials are responsible for protecting and overseeing the District's extracurricular cash assets, including extra-classroom activity fund money and athletic event admission collections. These responsibilities include adopting policies and procedures prescribing the records that District personnel and students must maintain and the duties and procedures that they must follow to adequately safeguard cash assets. Having good controls over these funds helps minimize the risk that errors or irregularities could occur and go undetected.

District officials need to improve their oversight of cash collections for extra-classroom activity funds and athletic events. Officials did not implement policies and procedures over athletic event admissions and adopt procedures to ensure adequate reconciliations of extracurricular cash collections activities were prepared. District officials did not ensure that sufficient documentation was maintained for cash collections and prenumbered cash receipts were issued for all the money collected. We identified 29 cash receipts totaling \$17,577 (15 extra-classroom activity receipts totaling \$12,327 and 14 athletic event fees totaling \$5,250) that were not deposited within the three-day period allowed by District policy. These funds were deposited from four to 15 days after they were received. In addition, the athletic director (Director) did not monitor or periodically reconcile the ticket inventory to account for the number of tickets sold. As a result of these discrepancies, District officials were unable to determine if all ticket money collected was deposited.

Extra-Classroom Collection Records

Generally, extra-classroom activity funds are raised by student activity organizations. Students raise and spend these funds to promote the general welfare, education and morale of all students and to finance the normal and appropriate extracurricular activities of the student body. The Regulations specify that the student treasurer of each activity fund shall maintain a ledger that shows all receipts and disbursements and indicates a daily running balance. This ledger should be in a form set by District officials. It is important for the faculty advisor to guide the student treasurer in posting the account ledger and periodically check the student treasurer's account balances. The student treasurers' ledgers must periodically be compared to the

central treasurer's ledger for accuracy and any discrepancies must be investigated and resolved.

Additionally, reconciliations should be prepared by an individual independent of the collection process and any discrepancies identified should be promptly investigated. In addition, cash collection should be limited to as few individuals as possible to reduce the risk of loss, theft or misappropriation.

Business office staff did not maintain a list of the extra-classroom central treasurers and faculty advisors charged with collecting and handling cash. In addition, District officials did not ensure sufficient documentation for extra-classroom cash collections was maintained, which made it difficult to reconcile cash collections and ensure that amounts collected were deposited intact.

We reviewed seven extra-classroom activity groups⁴ for the period July 1, 2014 through January 5, 2016 to determine if the activity fund student treasurers maintained ledgers showing all receipts and disbursements and kept a running balance that agreed with their central treasurer's ledger. We found that four activity group student treasurers did not maintain ledgers for the period reviewed. Student treasurers for three activity groups maintained adequate student ledgers, except for one minor discrepancy, which we discussed with District officials.

When we discussed extra-classroom reconciliation procedures with five of the District's central treasurers, only one central treasurer told us she reconciled student activities on a monthly basis, which involved sending an activity report to the group's student treasurer and faculty advisor to be signed and returned. When ledgers are not maintained or are not periodically reconciled with the central treasurers' records, there is an increased risk that fraud and concealment could occur and remain undetected.

Extra-Classroom Receipts

General Municipal Law requires every officer or employee who receives payment of money to issue a receipt to the person paying when no other evidence satisfactory for the purpose of audit is available. A consecutively prenumbered duplicate receipt form should be issued for any money received where other satisfactory evidence is unavailable. One copy should be provided to the customer and one copy should be retained for audit purposes. The office copy of issued receipt forms should be periodically reviewed by supervisory personnel, and any gaps or missing receipt forms should be investigated. Both copies of voided receipts should also be retained.

⁴ See Appendix C for information on our methodology.

While extra-classroom activity groups used deposit transmittal forms to remit money collected to the central treasurers (manually numbered using the cash receipt number from the electronic financial system), prenumbered receipts were not used by student treasurers to provide a form of receipt to those paying for extra-classroom group activities.

Because the Board did not ensure that District officials provided adequate oversight of cash receipts in accordance with the Regulations, District policies and good business practices, there is an increased risk that errors and irregularities could occur and remain undetected and that extracurricular money could be lost or misused.

Extracurricular Deposits

Good controls over cash receipts ensure that District officials supervise employees who handle cash and require that sequential, duplicate prenumbered receipts are issued for all cash collected. Additionally, District policy states that all cash received shall be secured in the vault until deposited with the business office or bank, which should occur within three business days of receipt; however, cash receipts in excess of \$500 shall be deposited within one day. Under no circumstances should money be left in classroom areas or desks.

We reviewed 117 extra-classroom cash receipts totaling approximately \$96,355 for seven extra-classroom activity groups and found that 15 cash receipts totaling \$12,327 were deposited from four to 13 days after being received by the central treasurers. Due to insufficient records showing when money was collected by the groups, we were unable to determine how long these funds were kept before being deposited with the central treasurers. Additionally, we reviewed athletic admissions and identified 14 deposits totaling \$5,250 that were deposited from four to 15 days after the events. When adequate records are not maintained to support cash receipts, District officials cannot ensure that cash receipts are deposited timely.

Athletic Event Admissions

When an admission fee is charged for an athletic event, prenumbered tickets should be used to determine the amount that should have been collected at the end of an event. Each ticket seller should promptly return all unsold tickets, the full amount of money collected and an accounting for the amount collected to the Director or the event coordinator.

We reviewed all athletic event admissions for the period July 1, 2014 through January 5, 2016 and found that the Director did not maintain a written record of all events where admissions were collected or a list of all individuals responsible for collecting cash. In addition, the Director told us he did not keep the ticket-taker reconciliation forms or the duplicate tickets sold during an event and monitor or

periodically reconcile the ticket inventory to account for the number of tickets sold.

To determine events where ticket money was collected, we reviewed the online athletic schedule and reviewed ticket-taker time sheets remitted to the business office. We identified 57 athletic events (individual games) and 38 deposit transmittal forms the Director remitted to the business office. For the remaining 19 events we found the following:

- The Director provided us with a list showing that three events required no ticket admission fees and no ticket-taker time sheets were remitted for these events.
- Ticket money collected for six charity games was not remitted to the business office and reconciliation documentation was not maintained.
- Ticket takers were paid by the District for 10 other events for which no deposits were made.

As a result of these discrepancies, District officials were unable to determine if all ticket money collected was deposited, and we could not determine if all ticket money was accounted for. Had District officials ensured event admission records and duplicate tickets from athletic events were maintained and periodically reconciled, they would have greater assurances that all money collected was accounted for.

Recommendations

District officials should:

3. Ensure adequate training is provided for all individuals who handle cash in the District and implement procedures to safeguard extracurricular cash resources.
4. Ensure adequate reconciliation documentation is maintained for all cash collections and that all cash collected for extracurricular activities is deposited in a timely manner.
5. Ensure prenumbered cash receipt forms are used, where no other form of evidence is available, to allow for adequate reconciliation.
6. Ensure that the student treasurers' ledgers are periodically reconciled and compared to the central treasurers' ledgers for accuracy. Any discrepancies should be investigated and resolved.

7. Develop policies and procedures for handling cash collections for athletic events.

Faculty advisors should:

8. Ensure that student treasurers maintain ledgers showing all receipts and disbursements and a running balance.
9. Ensure that the central treasurers receive supporting documentation for all activity fund cash receipts that are remitted for deposit and that the student treasurers properly account for all activity fund cash collected.

The Director should:

10. Monitor and periodically reconcile athletic event ticket inventory to account for the number of tickets sold.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following pages.

Pittsford Schools

Michael Pero
Superintendent of Schools

Administrative Offices
75 Barker Road – East Wing
Pittsford, NY 14534
585.267.1004
fax: 585.267.1088
Michael_Pero@pittsford.monroe.edu

July 14, 2016

Mr. Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614

Dear Mr. Grant:

On behalf of the administration and the Board of Education of the Pittsford Central School District, we express our appreciation for the opportunity to discuss and respond to the New York State Comptroller's Draft Audit Report for the period July 1, 2014 through January 21, 2016, here in referred to as, "the Report".

The report noted that the two objectives of the audit were:

1. Have District officials adequately safeguarded mobile computing devices (MCDs) to prevent unauthorized access to Personal Private Sensitive Information (PPSI)?
2. Have District officials provided adequate oversight of cash collections for extra-classroom activity funds and athletic events?

However, it is also important to note that during the approximately eleven (11) weeks of field work, your office reviewed numerous audit scope areas common in the OSC Reports in the last few years, however no findings were noted.

The District, while confident, was glad to hear the auditor's report that no fraud or malfeasance were noted and the above audited items did not glean findings of note. The District appreciated the auditor's comments and acknowledgement of the District's hard work on maintaining fiscal health, appropriately funded and use of reserves while staying within the Property Tax Cap. Such actions are more challenging for a district heavily dependent on the Tax Levy. The commendation of the Business Office professionalism and competency, despite the audit being performed during a time of integral staffing transition, is tantamount to the auditor's opinion expressed that the District is very transparent with its finances and provides the Board of Education and community "model information" for them

Michael Pero, Superintendent of Schools, Pittsford Central School District
Allen Creek Elementary • Jefferson Road Elementary • Mendon Center Elementary • Park Road Elementary • Thornell Road Elementary
Barker Road Middle School • Calkins Road Middle School • Pittsford Mendon High School • Pittsford Sutherland High School
www.pittsfordschools.org

to make informed decisions. The Board of Education, Administration and Business Office take the fiscal health of the District very seriously and embrace the need for strong fiscal oversight to protect the fiscal health and promote financial sustainability of the District and tax relief to the community.

On behalf of the Board of Education, the Assistant Superintendent and I feel it important to also provide you feedback on our audit experience by expressing our appreciation for the audit team that performed the field work. The team was very approachable, professional and thoughtful. It was refreshing to experience an audit where the audit team sat side by side with Business Office members and all worked collaboratively together to find multiple methods to examine the various scope areas. It was evident both parties were sharing information and auditing together, demonstrating the common goal of identifying improvement opportunities in a collaborative way. [REDACTED] and [REDACTED] have been invaluable to work with and their insights meaningful in preparing a thoughtful plan moving forward. As a result, this audit process has served as a useful tool for the District to examine various processes on a deeper level and scrutinize systems beyond the scope of the audit. Keeping internal controls, fiscal accountability and data security at the forefront of the District, not just select departments, is a culture that enhances the community's trust of the District and NYS. We appreciate the Comptroller's role in assisting the District in the continuous quest to enhance and adjust processes and systems in dynamic and challenging times.

This letter includes both the District's response as well as a high level corrective action plan. The corrective action plan was reviewed by the Audit Oversight Committee whose recommendation to the Board of Education was discussed and approved on July 12, 2016.

Audit Recommendations & District Response

Personal Private Sensitive Information (PPSI) on Mobile Computing Devices – during the Comptroller's review of the District's Information Technology and Data Information Systems, ALL of the more than 3,000 computers, laptops, iPads and smart phones were accounted for and quickly available for inspection. The District is pleased the measures it implemented as a result of the Comptroller's recommendation seven years ago are working.

***Audit Recommendation #1:** Adopt formal written policies and procedures to ensure a sound IT environment and protect PPSI on MCDs. These policies and procedures should outline the proper access, use and protection of PPSI on MCDs and address personally owned devices connecting to the District Network resources.*

District Response: As part of a regular review and updating of Board of Education Policies and Administrative Regulations the District started updating twenty-two (22)

policies and regulations in September 2015, prior to the OSC Audit notification. These policy updates are in various stages of completions with some complete and some being reworked to incorporate the written and verbal conversations of the OSC. We appreciate the OSC's acknowledgement that certain measures, such as encryption can pose significant expense and complexity and should therefore be approached thoughtfully. The District currently has several procedures to wipe/clean personal devices remotely if such devices are lost or stolen. The IT Department provides training on this topic through the District's new employee induction program, but will also provide recurrent training through department meetings and newsletters throughout the year.

***Audit Recommendation #2:** Ensure that a complete classification and inventory of PPSI stored on all District computer equipment is prepared to ensure data confidentiality, integrity and availability. The classification and inventory list should be updated on an ongoing basis, as appropriate to reflect any changes.*

District Response: As a result of the OSC's 2007 Audit recommendations, the District has performed two IT Security Audits, the last of which was in 2010 and focused primarily on physical security. The Chief Information Officer was glad to read this 2016 recommendation because it supported his proposal and quote to obtain independent third party services to review data security and perform a data inventory and classification report. The District is also seeking other costly options including but not limited to, processes for cloud rather than on device storage, such as One Drive and the widespread use of data encryption software. The District is moving forward under the following premise:

- Identify and classify the PPSI Data
- Identify how and where the PPSI Data is being stored
- Identify and address data storage weaknesses if they exist
- Develop Board of Education Policies and Administrative Regulations based on the above three bullets
- Implementation of Policies, Procedures and programs and equipment
- Provide all employees with education on what is and how to be more aware of PPSI and how best to work with it, what resources the District has available. (i.e., save data on the network not on MCD or e-mail attachment)
- PPSI Data Integrity is the responsibility of all employees and should NOT be on personal devices.

Extracurricular Cash Receipts and Athletic Event Collections – it is important to note some inherent differences between these two areas. While the prudent best practices of cash collection and deposits may be largely unilateral, **Extracurricular Accounts** are a totally separate entity “of the students for the students arms-length from the usual Business Office activities and separate from the District's General Fund”, (NYSED Pamphlet 2). **Athletic Event Collections or Admissions**, are a General Fund revenue to

support a taxpayer funded and operated program. Therefore, we will attempt to address the Audit Recommendations by these two distinct areas.

Extracurricular

***Audit Recommendation #3:** Ensure adequate training is provided for all individuals who handle cash in the District and implement procedures to safeguard extracurricular cash resources.*

District Response: The District annually provides training to all Extracurricular Advisors, Central Treasurers and Principals. Said training is provided by the District's Independent Auditor, Director of Finance/District Treasurer and Assistant Director of Finance. The district requires all Extracurricular club advisors to attend an annual training regardless of whether they normally handle cash or not. This training has traditionally been provided in a large group setting by the District's independent auditor. As is often the case with recurrent "seminar type" training, maintaining focus and urgency can be a challenge. Therefore the Business Office has or is working on measures to enhance advisor interaction in the learning through a scenario based instruction that will demonstrate the relevance of best practices and clearly demonstrate the advisor's ownership of prudent internal controls. These measures include:

- Requiring the Advisors themselves to write the responses to the Extracurricular Independent Audit Report as reviewed by the Audit Oversight Committee and Board of Education
- Developing an online training for Faculty Advisors with competency questions at the conclusion. This process would provide training assessment feedback, identify areas of understanding weaknesses and provide written evidence that the advisor has received the training and is competent to perform the duties of Faculty Advisor. This could also address potential training deficiencies in the rare instances when an interim Faculty Advisor is appointed due to the mid-year departure or leave of absence of the appointed Advisor.
- Working with the Human Resource Office on integrating formal and informal audit results in the Faculty Advisor selection process

***Audit Recommendation #4:** Ensure adequate reconciliation documentation is maintained for all cash collections and that all cash collected for extracurricular activities is deposited in a timely manner.*

District Response: Contrary to the Audit Report, the Business Office does keep records of all Faculty Advisors and Central Treasurers, through the use of Board of Education appointment records and collective bargaining agreements. As stated in the previous response, the Business Office assumes all Faculty Advisors are or could be "handling cash" and acts accordingly. For large fundraising events and recurrent activities, the Business Office keeps a calendar of events and reminds the Central Treasurer and Faculty Advisor to remit receipts to the District Treasurer if not received within three business

See
Note 1
Page 23

days. The Business Office has been in the process of investigating and implementing an Online Parent Payment Portal so parents can pay for items such as PSAT/SAT fees using their credit or debit card. The system will be a subset of the District's current successful program utilized by the School Lunch Program. Once implemented and we gain experience, we envision the rollout could be expanded to include the significant cash collection events of Extracurricular Clubs as well. This service should assist parents, provide more timely cash collections AND minimize handling of actual cash and the inherent risk that goes with it.

***Audit Recommendation #5:** Ensure pre-numbered cash receipt forms are used, where no other form of evidence is available, to allow for adequate reconciliation.*

District Response: The District Treasurer will continue to seek adequate cash receipt detail and Profit & Loss statements when cash is received. Considerable time is spent throughout the year assuring and obtaining adequate documentation and providing remedial training when necessary. The District also believes the Online Parent Payment Portal, when implemented, as stated above will assist with this endeavor.

***Audit Recommendation #6:** Ensure that the student treasurers' ledgers are periodically reconciled and compared to the central treasurer's ledgers for accuracy. Any discrepancies should be investigated and resolved.*

District Response: The District agrees that the best way to assure the integrity of the Central Treasurer is for the Faculty Advisor to provide oversight and encourage students to maintain financial records. This process fosters the student with the instructional opportunity of how to operate a club and is consistent with Board of Education Policy 5520. The Business Office will be recommending to the Audit Oversight Committee that the Internal Claims Auditor and/or the District Treasurer randomly and periodically spot review Club Treasurer and Central Treasurer records.

***Audit Recommendation #8:** Ensure that student treasurers maintain ledgers showing all receipts and disbursements and a running balance.*

District Response: See the District Response to Audit Recommendation #6

***Audit Recommendation #9:** Ensure that the Central Treasurers receive supporting documentation for all activity fund cash receipts that are remitted for deposit and that the student treasurers properly account for all activity fund cash collected.*

District Response: See the District Response to Audit Recommendation #6

Athletic Cash Collections and Event Admissions

Audit Recommendation #7: Develop policies and procedures for the handling of cash collections for athletic events

District Response: The District agrees with a statement from the Comptroller on page 11 of the Audit Report and believes it applies in this case, “cash collection should be limited to as few individuals as possible to reduce the risk of loss, theft or misappropriation”. As detailed in the Comptroller’s Report, currently there are several people involved and decisions are being made by those who may or may not be segregated from the cash process. Therefore, the District recommends handling Athletic cash receipts in a manner more aligned to Extracurricular Clubs and Musicals and in accordance with Board of Education Policy and NYSED Management Services Pamphlet 2. The recommended process will be:

- While planning the ensuing year’s general fund budget, the Athletic Director and Director of Finance will review the next year’s schedule of events to determine which events will charge admissions. This process after reviewing historical data will:
 - Enhance the integrity of historical data and strengthen the basis for which the administration can make decisions
 - Allow the Director of Finance to more accurately project Admissions Revenue
 - Allow the Director of Finance and Athletic Director to better plan and budget for related expenses such as ticket takers
 - The Business Office will have a schedule of events and will know ahead of time when to expect cash receipts and follow-up if receipts are not timely
- Ticket Takers will continue to be trained and provided rolls of pre-numbered tickets and a reconciliation sheet for them to complete and sign, as well as a sealed bank deposit bag. The Ticket Taker will:
 - Confirm on the sheet the amount of change funds received and initial
 - The ticket taker will affix the lowest ticket number
 - Upon completion of the event will affix the highest ticket number. The difference between the two numbers is the number of tickets sold, times the ticket price plus the change fund allocation should equal the amount of cash collected. Any over/short will be noted on the form and signed off by the Ticket Taker.
 - The Ticket Taker will place the reconciliation form and all cash in the sealing bank bag and personally deposit the bag in the main office drop safe
 - The next morning the District Courier (bonded) will collect the bag and deposit it at the District Office with the District Treasurer or receipt designee
 - The District Office through their segregation of duties process will count and reconcile all cash and reconciliation sheets and prepare a bank deposit
 - A summary report will be kept on file with the District Treasurer and forwarded to the Athletic Director for historical record keeping and assess if receipts were congruent to event participation

- If it is decided that an event will not charge admission, the decision, when practicable will be made in advance and communicated by the Athletic Director in writing to the District Treasurer
- The Assistant Superintendent for Business during the payroll certification process will spot check ticket taker time sheets to cash reconciliation records to assure that payment is consistent with services provided

Audit Recommendation #10: *The Athletic Director should monitor and periodically reconcile athletic event ticket inventory to account for the number of tickets sold.*

District Response: The District agrees with and will implement this recommendation. A periodic reconciliation of ticket inventory will be performed by district personnel independent of the sales and collection process.

Sincerely,

Michael Pero
Superintendent of Schools

Kim J. McCluski
President, Board of Education

APPENDIX B

OSC COMMENT ON THE DISTRICT'S RESPONSE

Note 1

While this information may have existed within various disparate records, it was not compiled into a centralized list, which would better aid District officials in providing adequate oversight.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objectives and obtain valid evidence, we performed the following procedures:

- We interviewed District officials to gain an understanding of the MCD environment and the cash collections process.
- We reviewed policies and procedures over IT and MCDs to identify the controls established. We also reviewed policies and procedures over cash collections to understand the controls over collections for athletic admissions and extra-classroom funds.
- We obtained an inventory of District-owned MCDs and judgmentally selected a percentage of MCDs according to various categories of users and used a random number generator to select a random sample of MCDs for review to determine if PPSI was present and if proper security features were in place to protect PPSI.
- We judgmentally selected and traced a sample of seven extra-classroom records from the central treasurers' records to deposits to ensure adequate documentation was maintained and reconciliations were performed in a timely manner for the period July 1, 2014 through January 5, 2016.
- We judgmentally selected and performed cash counts of five extra-classroom central treasurers.
- We traced athletic admissions documentation available to deposits for the period July 1, 2014 through January 5, 2016 to determine if deposits were made intact in a timely manner and adequately supported. We also used athletic event schedules and time sheets to assist in determining all events where collections were made for this analysis.

We conducted this performance audit in accordance with GAGAS. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX D

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
<http://www.osc.state.ny.us/localgov/>

APPENDIX E
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE

H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE

Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

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

GLENS FALLS REGIONAL OFFICE

Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin,
Fulton, Hamilton, Montgomery, Rensselaer,
Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE

Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE

Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange,
Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe,
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison,
Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS

Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313