New York State Comptroller
THOMAS P. DiNAPOLI

# Roosevelt Children's Academy Charter School

## Information Technology

**2025M-142 | April 2026**

**Division of Local Government and School Accountability**

# Contents

**Audit Results** . . . . . **1**

**Information Technology: Findings and Recommendations** . . . . . **3**

Finding 1 – School officials did not manage and monitor user access accounts. . . . . 3

Recommendation. . . . . 4

Finding 2 – School officials did not monitor employee Internet use or provide IT security awareness training. . . . . 5

Recommendations . . . . . 6

Finding 3 – The Director of Technology did not provide oversight of the consulting agreement with the IT vendor. . . . . 6

Recommendations . . . . . 7

Finding 4 – School officials did not create adequate IT policies. . . . . 7

Recommendations . . . . . 8

**Appendix A: Profile, Criteria and Resources** . . . . . **9**

**Appendix B: Response From School Officials** . . . . . **11**

**Appendix C: Audit Methodology and Standards** . . . . . **13**

# Audit Results

## Roosevelt Children's Academy Charter School

| Audit Objective | Audit Period |
|---|---|
| Did Roosevelt Children's Academy Charter School (School) officials adequately secure and protect information technology (IT) assets against unauthorized access, use and loss? | July 1, 2023 – March 20, 2025 |

### Understanding the Audit Area

School officials must secure and protect information technology assets to comply with certain New York State laws that mandate safeguards for personal, private, sensitive student/staff information (PPSI).[1] Protecting IT assets is crucial to maintain trust with students and families, as data breaches can lead to identify theft and loss of confidence in a school's ability to safeguard sensitive information. The cost associated with data breaches can be significant which can strain school budgets. Implementing a robust cybersecurity measure fosters a culture of security awareness among staff and students. Continuous training helps prevent accidental breaches, which are often caused by human error. By prioritizing the security of IT assets, schools can protect sensitive information, comply with legal requirements, maintain trust, and avoid financial repercussions.

In fiscal year 2024, the School paid an outside IT vendor $158,102 to provide IT services, for managing the network and computers for the entire School. Additionally, the vendor was responsible for the School's servers, firewall and all IT equipment and managed all user accounts and permissions. The School had 248 enabled network user accounts.

## Audit Summary

School officials did not establish adequate controls to secure and protect IT systems and assets against unauthorized access, use and loss. As a result, School officials cannot be assured that the School's IT systems are secured and protected against unauthorized access, use and loss, and there is an increased risk that the School could lose important data and suffer a serious interruption in operations.

School officials have not implemented comprehensive procedures for managing and monitoring user access to the School's network and computers. Because there are no written procedures to document,

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third-parties or other individuals or entities.

authorize or confirm user account changes, 51 unneeded accounts went unnoticed. When unneeded user accounts remain enabled, the School has an increased risk that disgruntled employees or attackers could use these accounts as entry points to access PPSI and compromise IT resources.

Although School officials set up web-filtering software to restrict obscene materials and unlawful activity based on website category, they did not monitor employee Internet use. We reviewed Internet histories on 14 School employee computers and determined that nine employees used the computers to access websites for personal use, such as entertainment, personal finance, email, shopping, travel and other miscellaneous personal use. One of these users conducted personal business activities using the School computer. In addition, School officials did not provide IT security awareness training to help ensure employees understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the School's IT systems.

Although the Director of Technology was responsible for overseeing the services provided by the IT vendor, School officials did not have procedures to monitor and review the services performed by the IT vendor. The Director of Technology was unable to provide documentation related to the monitoring of the IT vendor's compliance with the consulting agreement. In addition, the Board of Trustees (Board) did not develop adequate IT policies or procedures.

Weaknesses in oversight, other internal controls and policies increase the risk that hardware or software systems may be lost, damaged or compromised by unauthorized or inappropriate access and use.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes 12 recommendations that, if implemented, will improve the School's IT security and protect systems against unauthorized access, use and loss. School officials generally agreed with our findings and indicated they plan to initiate corrective action.

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. Our methodology and standards are included in Appendix C.

The Board has the responsibility to initiate corrective action. We encourage the Board to prepare a written corrective action plan (CAP) that addresses the recommendations in this report and forward it to our office within 90 days. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Board to make the CAP available for public review.

# Information Technology: Findings and Recommendations

School employees and officials use school-owned IT assets (e.g., computers and laptops) to perform day-to-day operations and assess and store information collected by the school. If an IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and rebuild.

Unmanaged network and local user accounts are potential entry points for attackers and other unauthorized individuals, and if compromised, the lack of a contingency plan can paralyze a school's operations. School officials should develop and implement written procedures for periodically reviewing enabled network user accounts to ensure they are still needed and disabling nonstudent network user accounts as soon as they are no longer needed.

IT security awareness training should explain rules of behavior for using the Internet, a school's financial application and the network, and communicate related policies and procedures to all IT users. IT security awareness training educates system users on best practices, such as identifying phishing attempts and using strong passwords, significantly reducing the likelihood of a security incident caused by a cyber-attack or inadvertent human error.

A school board should monitor and ensure compliance with consulting agreements with the school's vendors to address the specific needs and expectations for IT services. Consulting agreements should also be periodically reassessed, especially when a school's IT environment or needs change significantly. Providing oversight of the consulting agreement with the IT vendor helps to ensure a school's IT security objectives are met.

IT security policies describe the tools and procedures used to help protect IT systems, including data and networked applications, and help define the expectations for appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for a school board to adopt, update and distribute policies for key IT security issues to help safeguard against unauthorized access, use or loss. The school board should periodically review IT policies, update them as needed and establish who is responsible for monitoring compliance with these policies. These measures are essential components of a robust cybersecurity posture, which is vital for effective and responsible governance, and helps safeguard against financial loss and ensure critical functions are not interrupted.

More details on the criteria used in this report, as well as resources we make available to school officials that can help officials improve operations (Figure 3), are included in Appendix A.

## Finding 1 – School officials did not manage and monitor user access accounts.

School officials have not implemented comprehensive procedures for managing and monitoring user access to the School's network and computers. The School's IT vendor configured and maintained the School's IT environment, which included servers, desktops, network accounts and software applications. The School's Human Resources specialist is responsible for providing employee-status information to either the Director of Technology or the IT vendor to make any necessary changes.

We reviewed the School's 248 enabled network user accounts and determined 51 user accounts were unneeded and should have been disabled. Specifically, we identified accounts for:

- Seven users who accepted an offer of employment with the School but were never actually employed.
- One user who received a new account due to a name change but the old account was never disabled.
- Two users for which School officials could not provide an explanation.

There were also 41 user accounts assigned to former School employees who had left employment going back as far as 2016 (Figure 1). Upon sharing the results of our testing, the IT vendor immediately disabled the accounts.

**Figure 1: Enabled User Accounts of Former Employees, By Year of Separation**

| Year | Number of User Accounts |
|---|---|
| 2016 | 1 |
| 2017 | 13 |
| 2018 | 2 |
| 2019 | 3 |
| 2020 | 2 |
| 2021 | 2 |
| 2022 | 3 |
| 2023 | 8 |
| 2024 | 7 |

Because there are no written procedures to document, authorize or confirm account changes, these unneeded accounts went unnoticed. When unneeded user accounts remain enabled, the School has an increased risk that disgruntled employees or attackers could use these accounts as entry points to access PPSI and compromise IT resources.

Of particular risk are the network user accounts created for individuals that were offered positions at the School, but were never actually employed. Without adequate account management, the School has an increased risk that attackers could successfully compromise its IT system. Also, because user accounts were not monitored, there was a greater risk that officials would not notice whether the accounts had been compromised or used for malicious activities, which could give attackers more time and opportunities to access PPSI and compromise IT resources.

## Recommendation

School officials should:

1. Develop comprehensive written procedures for monitoring and managing user accounts that include periodically reviewing user access and disabling or changing accounts when access is no longer needed.
2. Ensure access rights are based on need consistent with assigned job duties and responsibilities and that access is removed upon termination of employment.

## Finding 2 – School officials did not monitor employee Internet use or provide IT security awareness training.

Although officials set up web-filtering software to restrict obscene materials and unlawful activity based on website category, they did not monitor employee Internet use. The School's acceptable use policy (AUP) states that School IT assets, including computers, electronic mail and voice mail, should only be used for conducting School business. However, the AUP also states that incidental and occasional personal use of School computers, electronic mail and voicemail systems is permitted. Because the wording in the AUP is vague, employees are left to interpret and determine what is reasonable incidental and occasional personal use.

We reviewed the Internet history on 14 School computers assigned to 14 employees and determined that nine computers were used to access websites for personal use. In addition, using one of the nine School computers, one user conducted personal business activities (Figure 2).

**Figure 2: Examples of Personal Internet Use**

| Type | Website |
|---|---|
| Entertainment and News Media | vibe.com, bossip.com, tmz.com, youtube.com, nypost.com, cbsnews.com, nytimes.com |
| Financial, Email and Shopping | bankofamerica.com, paypal.com, westernunion.com, jcpenney.com, etsy.com, macys.com, aol.com, mail.yahoo.com, mail.google.com |
| Gambling | fanduel.com |
| Miscellaneous Personal Use | citypay.nyc.gov, guns.com, brooklynfare.com, cardgames.io, sudoku.com, opentable.com, ubereats.com, chownow.com |
| Personal Business | counter.com, taxwise.com, hrblock.com |
| Social Media | facebook.com, instagram.com, tiktok.com |
| Travel | expedia.com, jetblue.com, hilton.com |

While web-filtering software can help mitigate instances of inappropriate and/or personal Internet browsing, periodic reviews of Internet history would provide a more definitive review of activity to identify inappropriate and/or personal Internet browsing. Unauthorized Internet browsing and personal use of School computers increases the likelihood of exposing computer systems to malicious content that could compromise PPSI or the IT system.

In addition, School officials did not provide IT security awareness training to help ensure employees understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the School's IT systems.

The School has a security awareness training policy which states security awareness training is offered by the School twice annually and must be completed by users once every 12 months. School officials stated that they did not provide the mandatory security awareness training for users for the 2024 school year. In the 2023 school year, the security awareness training was sent out to 123 users, but only 10

users completed the course. Officials were unaware that the security awareness training should be provided to users on a routine basis and did not enforce or require the training to be completed.

When security awareness training is not provided or completed, there is an increased risk that users will not understand their responsibilities, putting the School's data and IT systems at greater risk for unauthorized access, misuse or abuse. As a result, the School has an increased risk that it could lose important data and suffer a serious interruption in operations.

## Recommendations

School officials should:

3. Implement procedures to monitor employee Internet use and ensure compliance with IT policies.
4. Ensure IT security awareness training is periodically provided to all individuals who use School IT resources.

## Finding 3 – The Director of Technology did not provide oversight of the consulting agreement with the IT vendor.

The School has a consulting agreement with an IT vendor that is adopted by the Board annually and solely reviewed and signed by the Chief Financial Officer (CFO). The most recent Board-adopted consulting agreement was dated July 2024. The scope of services provided include hardware monitoring and maintenance, network and help-desk support, anti-virus/malware protection and file-server hosting. The consulting agreement further states that the IT vendor will provide the School with network and end-user device monthly activity reports in electronic format.

Although the Director of Technology was responsible for overseeing the services provided by the IT vendor, School officials did not have procedures to monitor and review the services performed by the IT vendor. The Director of Technology was unable to provide documentation related to monitoring the IT vendor's compliance with the consulting agreement.

In addition, because the Director of Technology was not involved in the adoption of the annual agreement, she was unaware that the IT vendor should be providing activity reports. The IT vendor told us he has the reports, but School officials have never requested them. Therefore, the IT vendor does not provide periodic activity reports to the Director of Technology or the Board. Instead, issues are communicated as they arise. As a result, officials could not ensure that the School's network and financial software data was adequately safeguarded.

## Recommendations

The CFO should:

5. Ensure that the consulting agreement addresses the School's specific needs and expectations for IT services.

6. Ensure the Director of Technology is included in the consulting agreement renewal process.

School officials should:

7. Establish procedures for monitoring and reviewing the services provided by the IT vendor.

The Director of Technology should:

8. Monitor the IT vendor's compliance with the consulting agreement.

9. Request and review monthly activity reports from the IT vendor.

## Finding 4 – School officials did not create adequate IT policies.

The Board did not adopt any written policies, procedures or guidelines related to user account management procedures, patch management or passwords. Instead, School officials and employees are provided with an employee manual which includes general policies related to the use of School technology, social media and computer security. The current version of the employee manual is dated August 2024 and was originally adopted by the Board in May 2024.

Although School officials indicated that the School maintains an AUP, officials were unable to provide proof of Board adoption. The AUP states that any employee who violates the AUP by using the electronic communication systems for improper purposes may be subject to discipline, up to and including termination, but it does not provide examples of improper use. The Director of Technology stated that School officials ensure that employees sign the employee AUP acknowledgement form agreeing to follow the policies outlined. However, there is no regular screening or monitoring being performed on user accounts outside of the monitoring performed by the IT vendor. The Director of Technology also stated that there were other controls such as web filters, including the restriction of web mail, so users cannot access the websites which have been blocked. However, these controls cannot be used for monitoring to verify compliance. Because School officials did not monitor employee Internet use, they could not determine whether employees were complying with the School's AUP or, if applicable, when disciplinary action was appropriate.

While comprehensive policies will not guarantee the safety of IT systems, the failure to adopt appropriate policies significantly increases the risk that users will not understand their responsibilities, putting the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse.

## Recommendations

The Board should:

10. Adopt adequate IT policies and procedures (e.g., user account management procedures, patch management and passwords).

11. Update existing IT policies to clearly define acceptable use and what is allowed and what is prohibited activity.

School officials should:

12. Implement procedures to periodically monitor compliance with adopted IT policies.

# Appendix A: Profile, Criteria and Resources

## Profile

The School, located in the Town of Hempstead, in Nassau County, is governed by an eight-member Board responsible for the School's general management.

The Board is responsible for general oversight of the School's operations and educational affairs, which includes maintaining security over the School's IT system. School officials contract with a third-party vendor for IT services including support, network management and other services.

The School has 139 employees, 248 enabled user accounts and 1,264 enabled network computer accounts (e.g., servers, desktops, and laptops).

## Criteria – Information Technology

Although no single practice or policy on its own can adequately safeguard IT systems from cybersecurity risks, there are several IT governance efforts that, if properly enacted and monitored, collectively increase the odds IT systems will remain safe.

User accounts enable networks and computers to recognize specific users, grant appropriate user permissions and provide user accountability by associating user accounts with specific users. School officials are responsible for restricting user access to only those applications, resources and data needed to complete job duties and responsibilities. This helps ensure IT data and assets are protected from unauthorized use and/or modifications. When employees leave School employment or when user accounts are no longer needed, these user accounts should be disabled in a timely manner. School officials should develop written procedures for granting, changing and removing user access and permissions to the overall networked computer system and to specific computers, applications and folders.

The School adopted an employee manual specifying the acceptable and prohibited use of the School's technology. The Board should ensure improper use is clearly defined and that officials monitor employees' computer use to ensure they comply with the School's AUP. Monitoring for compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Automated mechanisms, such as web-filtering software, may be used to perform this process and can help security professionals routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt at unauthorized access.

The School adopted a security awareness training policy requiring users to complete IT security training annually. To help minimize the risk of disruption, officials should have periodic IT security awareness training that explains common security threats and the proper rules of behavior for using the Internet

and IT resources, systems and data. The training should communicate policies and procedures to all IT system users, so they understand IT security measures and their roles in safeguarding data and IT assets.

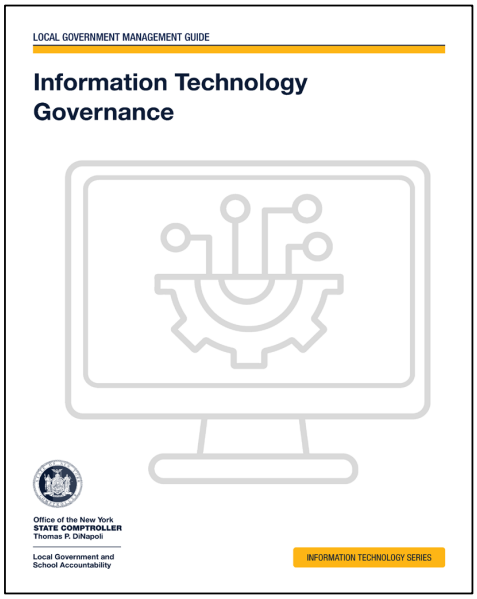
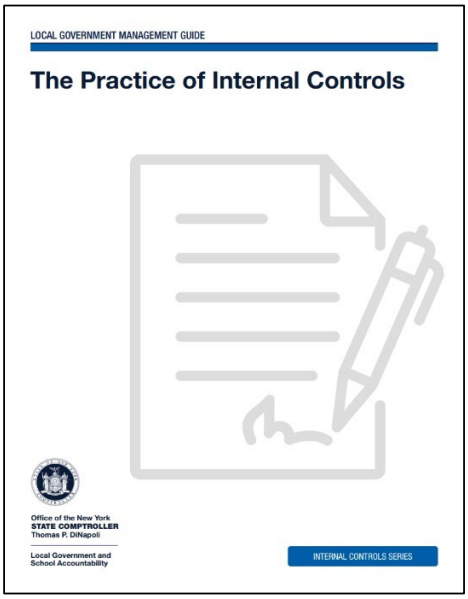
The Board adopted an annual consulting agreement with the School's IT vendor. Consulting agreements should be reviewed by a school's legal counsel and IT staff, as appropriate.

A board should provide oversight and leadership by adopting IT policies that consider people, processes and technology. These policies should be communicated to all IT system users and include procedures to ensure compliance. This helps reduce the risk of data, hardware and software being lost, damaged or compromised by unauthorized access and misuse.

## Additional Information Technology Resources

**Figure 3: OSC Publications**

OSC *Local Government Management Guides* and other informational resources are available on our website to help officials understand and perform their responsibilities.

| *Information Technology Governance* | *The Practice of Internal Controls* |
|---|---|
|  |  |
| https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf | https://www.osc.ny.gov/files/local-government/publications/pdf/the-practice-of-internal-controls.pdf |

In addition, our website can be used to search for audits, resources, publications and training for officials: https://www.osc.ny.gov/local-government.

# Appendix B: Response From School Officials



**From the Desk of Jacqueline Jean-Francois**

April 8, 2026

Comptroller Thomas P. DiNapoli

New York State Office of the State Comptroller

Division of Local Government and School Accountability

110 State Street, 11th Floor

Albany, NY 12236

**Re: Acknowledgment of Draft Report — Examination 2025M-142 | Audit Period: July 1, 2023 – March 20, 2025**

Dear Comptroller DiNapoli,

Roosevelt Children's Academy Charter School confirms receipt of the draft Report of Examination 2025M-142, reviewed with school leadership on March 26, 2026.

We accept the findings as presented. The audit identified gaps in our IT governance, including user account management, internet oversight, staff training, vendor monitoring, and policy structure. These conditions existed at the time of the audit and are not in dispute.

On March 24, 2026, the Board of Trustees approved a comprehensive Information Technology Policy and Procedures Manual. This framework addresses each of the twelve recommendations outlined in the draft report.

A mandatory cybersecurity training program is now in place, and vendor oversight procedures are active with ongoing reporting.

These actions were underway during the audit period and were

completed before this correspondence.

Because the report remains in draft form, we will submit our Corrective Action Plan upon issuance of the final report. Please notify us when it is released so we may meet the required 90-day timeline.

We remain available to support any follow-up review and can provide all supporting documentation upon request.

Respectfully submitted,

**Jacqueline Jean-Francois**
Director of Technology & Data Protection Officer

**Reginald Tuggle**
Chair, Board of Trustees

cc: Philip Leconte, CFO/COO — Douglas Thomas, IT Consultant — Board of Trustees

# Appendix C: Audit Methodology and Standards

We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed School officials and employees to obtain an understanding of the School's IT operations and related policies and procedures and to determine whether the policies and procedures were adequate, and School employees received IT security awareness training.
- We analyzed and assessed all 248 enabled network user accounts using a computerized audit script we ran on March 20, 2025, and compared the network user accounts to the School's organizational chart to determine whether there were any enabled network user accounts assigned to former School employees.
- We reviewed the consulting agreement between the School and IT vendor, and all invoices paid to the IT vendor during the audit period to identify the services provided. We interviewed School officials to determine whether the services identified were provided and compliance with the agreement was monitored.
- We reviewed the School's employee manual and AUP providing guidance to officials and employees on acceptable and prohibited computer use.
- We used our professional judgment to select 14 computers based on the job titles and duties of the School officials and employees who had access to these computers. We reviewed signed AUP acknowledgement forms on file at the School for the sample of 14 computers' assigned users. The officials and employees using these computers had access to the School's accounting software and employee and student PPSI. We ran a computerized audit script on the 14 computers on March 19 and 20, 2025, and reviewed the Internet history to determine whether School officials and employees accessed secured and appropriate websites.
- We physically observed the School's IT assets to determine whether the School implemented appropriate 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 generally accepted government auditing standards (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 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.

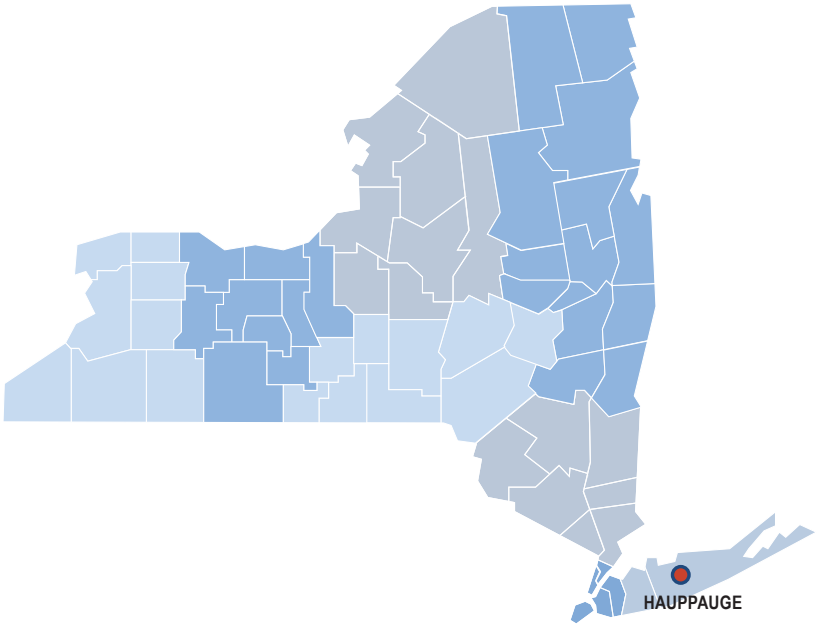
## Contact

**HAUPPAUGE REGIONAL OFFICE** – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties




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

https://www.osc.ny.gov/local-government

Local Government and School Accountability Help Line: (866) 321-8503