New York State Comptroller
THOMAS P. DiNAPOLI

Glen Cove City School District

Information Technology

June 2026 | 2025M-144

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Glen Cove City School District

Audit Objective

Did Glen Cove City School District (District) officials adequately manage nonstudent network user accounts?

Audit Period

July 1, 2023 – May 14, 2025

Understanding the Audit Area

School district officials must manage network user accounts to help protect personal, private, sensitive student/staff information (PPSI),[1] including (but not limited to) student and employee names, dates of birth, addresses, medical information and social security numbers. Network user accounts are potential entry points for attackers and, if compromised, could be used to make unauthorized changes to official school district records and deny legitimate access to network resources. Proper network user account management can help safeguard against events that could have criminal, civil, regulatory, financial and reputational impacts on school district operations.

As of May 14, 2025, the District had 1,104 enabled nonstudent network user accounts.

Audit Summary

District officials did not adequately manage nonstudent network user accounts. As of May 14, 2025, 296 of the District's 1,104 enabled nonstudent network user accounts (27 percent) were not needed and should have been disabled. Additionally, six unneeded nonstudent network user accounts had administrative permissions. Unneeded network user accounts, including those with elevated administrative permissions, are additional entry points into a network and, if compromised by an attacker, could be used to inappropriately access the District's network to view and/or remove personal information accessible by that compromised network account; make unauthorized changes to District records; or deny legitimate access to the District network and records.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes six recommendations that, if implemented, will improve the District's management of nonstudent network user accounts and permissions. District officials 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 Article 3 of the New York State General Municipal Law. Our methodology and standards are included in Appendix C.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of the New York State General Municipal Law, Section 2116-a (3)(c) of the New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more

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.

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 CAP should be posted on the District's website for public review.

Information Technology: Finding and Recommendations

School district officials should develop and implement written procedures for granting, changing and disabling nonstudent network user account access to the network. Procedures should establish a process for revoking access by immediately disabling nonstudent network user accounts when they are no longer needed. In addition, school district officials should regularly review enabled nonstudent network user accounts to ensure they are still needed and disable unnecessary or unneeded user accounts.

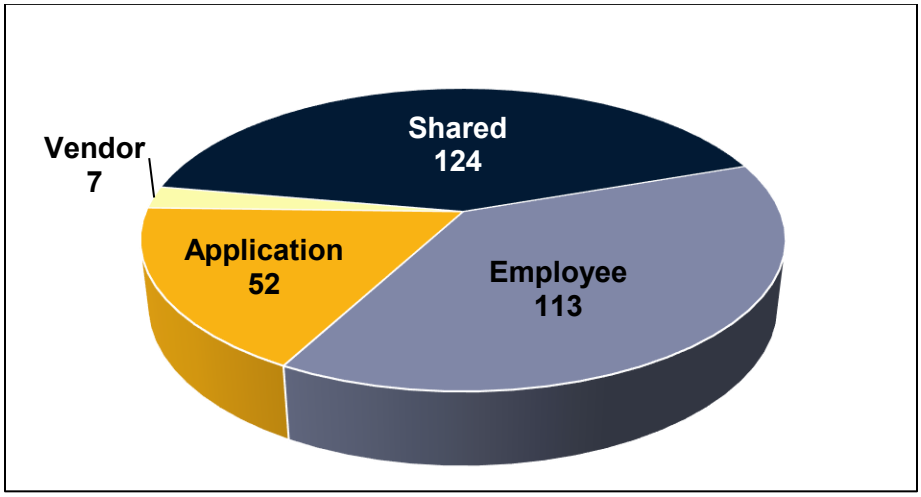
Nonstudent network user accounts include accounts assigned to school district employees, vendors, shared accounts and application accounts.[2] When nonstudent network user accounts are not properly managed, there is an increased risk for unauthorized access to a network and unauthorized use of PPSI.

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

Finding 1 – District officials did not adequately manage nonstudent network user accounts and permissions.

District officials did not adequately manage nonstudent network user accounts to ensure all accounts and their permissions were needed. We reviewed all 1,104 enabled nonstudent network user accounts as of May 14, 2025, and determined that 296 user accounts (27 percent) were not needed and should have been disabled (Figure 1). Additionally, six unneeded application nonstudent network user accounts had administrative permissions that were not needed. Users with administrative privileges can perform activities that include creating new network user accounts and manipulating the security settings configured on the network. Unnecessary administrative permissions could be misused for malicious activities.

Figure 1
Unneeded Nonstudent Network User Accounts



2 Shared accounts are accounts that are used by more than one user for the purpose of logging into a computer system and accessing network resources. For example, shared accounts may be used for testing purposes, training purposes or for shared e-mail accounts, such as a service helpdesk account. Application accounts are accounts that include software accounts, software service accounts, and devices such as Point of Sale, printers, etc.

Shared Accounts – We determined that 124 of the 139 enabled shared user accounts (89 percent) were not needed and should have been disabled, including 72 accounts that were not logged into since their creation as long as 20 years ago and 36 accounts that were not logged into since at least 2023. IT department staff acknowledged that 123 of these shared user accounts should not have been enabled. IT department staff could not explain why the remaining one shared user account remained enabled but believed it may have been used by individuals in the District's teachers' association based on the account name. However, we determined that this account was not logged into after it was created in April 2014 and was likely not needed and should have been disabled.

Employee Accounts – We determined that 113 of the 823 enabled employee user accounts (14 percent) were not needed and should have been disabled. IT department staff told us that 108 employee user accounts were assigned to former District employees and five employee user accounts were unnecessary duplicate accounts. Of the 108 user accounts assigned to former District employees, 44 accounts were not logged into since their creation as long as 20 years ago and 41 accounts were not logged into since at least 2023.

Application Accounts – We determined that 52 of the 110 enabled application user accounts (47 percent) were not needed and should have been disabled. For example, two application accounts were active despite not being used for over five years. IT department staff told us that these 52 application user accounts were unnecessary. Furthermore, six of the unneeded application user accounts had administrative permissions.

Vendor Accounts – We determined that seven of the 32 enabled vendor accounts (22 percent) were unneeded and should have been disabled. IT department staff told us that these seven accounts were assigned to former consultants, such as a special education consultant and two certified trainers, and were no longer needed.

Although the District had three different Assistant Superintendents for Curriculum, Instruction and Technology (Assistant Superintendents) responsible for the administrative oversight of the IT department since July 2021, they did not establish written procedures for granting, changing and disabling nonstudent network user account access. The District Coordinator for Instructional Technology (Coordinator) could not explain why the 296 unnecessary nonstudent network user accounts, including those with administrative permissions, remained enabled. Additionally, the Coordinator told us that nonstudent network user accounts were managed by the former Systems Administrator until May 2024. The District then contracted with the Nassau Board of Cooperative Educational Services (BOCES) to take over the Systems Administrator's role in June 2024, including managing nonstudent network user accounts. However, IT department staff told us that, because the Nassau BOCES staff prioritized other issues with the District's IT environment, they did not actively manage nonstudent network user accounts and permissions.

Unneeded nonstudent network user accounts, including those with administrative permissions, are additional entry points into a network and, if compromised by an attacker, could be used to inappropriately access the District's network to view and/or remove personal information accessible by that compromised account; make unauthorized changes to District records; or deny legitimate access to the District network and records. An attacker could use these additional entry points to severely disrupt District operations by:

- Denying District employees access to information they need to perform their job duties.
- Installing malicious software that could cripple and/or completely shut down the District's network.
- Obtaining and publicly releasing PPSI accessible to a compromised nonstudent network user account which could be used to facilitate identity theft.

Additionally, when a school district has many enabled network user accounts that must be managed and reviewed, it could make unneeded account detection less timely, and accounts could be inadvertently granted unneeded permissions.

Recommendations

The Assistant Superintendent should:

1. Develop written procedures for granting, changing and disabling nonstudent network user accounts.

2. Ensure that the IT department and Nassau BOCES staff adhere to District policies and procedures.

3. Establish clear roles and responsibilities for IT department and Nassau BOCES staff and clearly communicate them to those responsible for managing nonstudent network user accounts.

The Coordinator should ensure that Nassau BOCES staff:

4. Disable nonstudent network user accounts of employees and vendors when they separate from the District, and disable unneeded shared and application user accounts in a timely manner.

5. Evaluate all current nonstudent network user accounts, including those with administrative permissions, and disable those that are not needed.

6. Periodically review all nonstudent network user accounts for necessity and appropriateness.

Appendix A: Profile, Criteria and Resources

Profile

The District is located in the City of Glen Cove in Nassau County and educates approximately 3,082 students. The District is governed by the elected seven-member Board of Education (Board) responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer and is responsible for the District's day-to-day management under the Board's direction.

The District's IT department is managed by the Coordinator, who oversees the IT department's daily work and the Nassau BOCES engineers responsible for network maintenance. The Assistant Superintendent provides administrative oversight of all IT within the District. The Systems Administrator was responsible for managing nonstudent network user accounts until May 2024, and Nassau BOCES engineers assumed the responsibilities in June 2024.

Criteria

Nonstudent network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access, and loss. Nonstudent network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view PPSI on the network, make unauthorized changes to official school district records or deny legitimate access to network resources.

Nonstudent network user accounts with administrative permissions have oversight and control of the network, with the ability to add new users and change users' passwords and permissions. Users with network administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. Therefore, school district officials should limit users with administrative permissions and regularly monitor all user account access to ensure it is appropriate and authorized.

School district officials should limit the use of shared and application network user accounts because they are not linked to one individual and officials may not be able to hold users accountable for their actions when using these accounts. Shared user accounts have usernames and passwords that are shared among two or more users and are often used to provide access to guests or other temporary or intermittent users. IT staff often use service accounts to run particular network or system services or applications (e.g., automated backup systems). School district officials should routinely evaluate the need for the accounts and disable those that are not related to a current district or system need.

School district officials should develop and implement written procedures for granting, changing and disabling nonstudent network user account access to the network. Procedures should establish a process for revoking access by immediately disabling nonstudent network user accounts when they are no longer needed. To minimize the risk of unauthorized network use, access and loss, school district officials should actively manage nonstudent network user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are needed. When nonstudent network user accounts are no longer needed, they should be disabled in a timely manner. One way to help accomplish this is to establish and implement a system in which nonstudent network user accounts are automatically disabled after a reasonable specified period without a valid user account login, unless explicitly authorized to remain enabled on the network for an ongoing district or system need. In addition, school district officials should regularly review enabled nonstudent network user accounts to ensure they are still needed and disable unnecessary or unneeded user accounts.

Additional Resources

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

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

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

Appendix B: Response From District Officials

The content below is a reproduced copy of the original response letter issued by District officials and is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[3] and may have included changes to spelling and grammar. The substance of the content was not changed.

GLEN COVE SCHOOLS
154 DOSORIS LANE • GLEN COVE, NEW YORK 11542 • 516-801-7010 • FAX: 516-801-7019

Dr. Alexa Doeschner
Superintendent of Schools
adoeschner@glencoveschools.org

Mr. Ira McCracken, Chief of Municipal Audits
Office of the New York State Comptroller
Hauppauge Regional Office
NYS Office Building Room 3A10
250 Veterans Memorial Highway
Hauppauge, NY 11788-5533

May 1, 2026

Dear Mr. McCracken,

The Glen Cove City School District has received and reviewed the draft of the Information Technology (2025M-144) audit report. This audit report reviewed the District's management of nonstudent network user accounts. This letter serves as our official response to the audit findings. We agree with your findings and are currently working on a formal corrective action plan to implement your recommendations.

The District would like to thank the Comptroller's Office for their professionalism and collaboration during this audit, and we appreciate the opportunity to enhance and improve our operations.

Respectfully,

Dr. Alexa Doeschner

3 https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule

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 reviewed District IT policies and procedures and interviewed the former and current Coordinator and Nassau BOCES staff to gain an understanding of the District's IT operations, including the management of nonstudent network user accounts.

- We ran a computerized audit script on the District's network on May 14, 2025. We analyzed the script results to obtain information about the District's 1,104 enabled nonstudent network user accounts (including their permissions) to determine whether the accounts were necessary and appropriate. We compared all 1,104 enabled nonstudent network user accounts to a current employee list. For user accounts that were not assigned to a specific employee, we followed up with District officials to determine the purpose of the user account (i.e., vendor, shared and application accounts). We analyzed the account login dates to identify unused and possibly unneeded nonstudent network user accounts.

- We followed up with the current Coordinator, the Assistant Superintendent and Nassau BOCES staff to discuss possible unneeded nonstudent network user accounts and to determine why unneeded accounts remained enabled on the network.

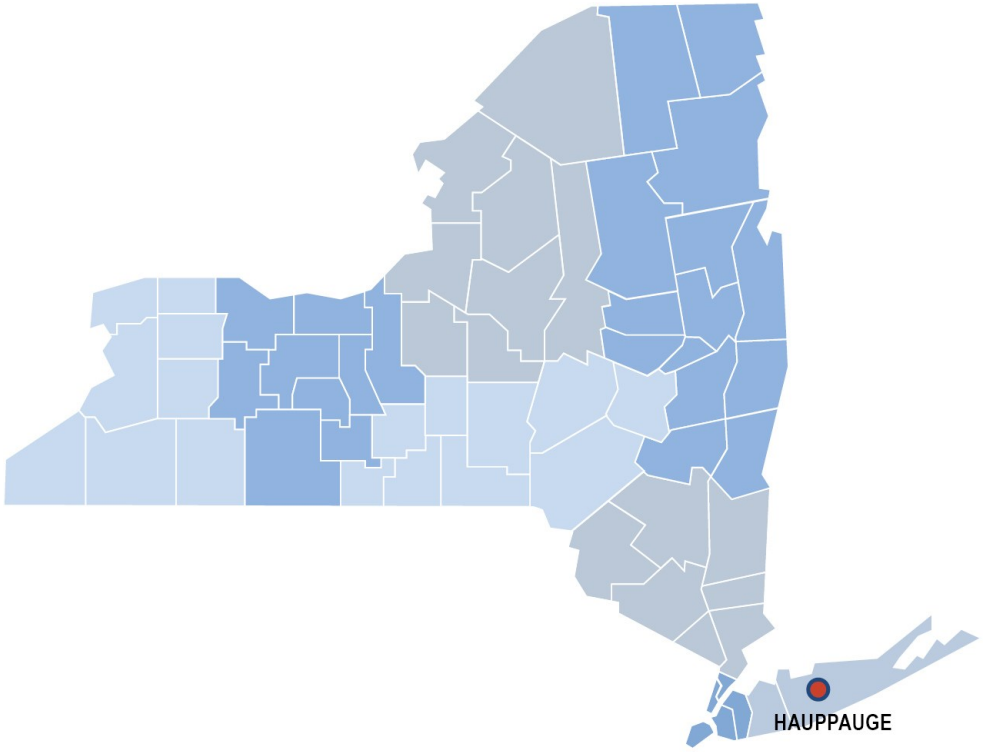
Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted 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.

Questions?

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



Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability