New York State Comptroller
THOMAS P. DiNAPOLI

Malverne Union Free School District

Building Access

August 2026 | S9-26-6
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Malverne Union Free School District

Audit Objective

Did Malverne Union Free School District (District) officials properly manage and monitor building access accounts and devices?

Audit Period

July 1, 2024 – November 30, 2025

We extended our audit period to April 21, 2026 to review access activity logs.

Understanding the Audit Area

Building access controls are essential for enhancing security and enabling school officials to manage and monitor entry points within educational institutions. These systems authenticate a user through devices such as key fobs, key cards, badges, or similar technologies, helping to ensure only authorized individuals can enter school buildings. By limiting access in this way, schools can better safeguard their facilities and maintain a safe and secure environment for students, teachers, staff and visitors.

The District utilizes a building access management system (system) with 420 active building access accounts (accounts), including 351 devices issued to current employees and 69 issued to non-employees, of which 24 are shared devices.[1] Each of the District's five school buildings have a single public point of entry. Employees may also access the buildings through additional secured entry points, which require a device for entry.

Audit Summary

District officials did not properly manage and monitor building access accounts and devices (key cards). As a result, there was a potential risk for unauthorized access to District school buildings, compromising building security and safety for students, teachers, staff and visitors. Specifically, the District had active, but unneeded, accounts with assigned key cards in the system:

- 17 individual non-employees had duplicate active key cards that District officials could not locate, including nine which were never used.
- Nine shared key cards that District officials could not locate and were never used.

Although District officials had a process for adding accounts in the system for employees and non-employees, no one periodically reviewed active accounts to determine whether they were needed, which is why officials did not recognize 18 active key cards with no activity were unneeded. Furthermore, these issues occurred because District officials did not develop written policies and procedures that clearly assign roles and define the responsibilities for managing and monitoring accounts or issuing key cards.

This report includes three recommendations that, if implemented, will help District officials improve management and monitoring of building access accounts and key cards.

1 A shared account or device is assigned to a user for a specific role or function but not assigned to a specific individual (e.g., vendors or first responders).

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the Office of the State Comptroller's (OSC's) authority as set forth in Article 3 of New York State General Municipal Law (GML). The audit's 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 OSC within 90 days, pursuant to Section 35 of GML, 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 information on preparing and filing the CAP, please refer to the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The CAP should be posted on the District's website for public review.

Building Access: Finding and Recommendations

Properly managing and monitoring building access is a fundamental security function and the responsibility of school district officials. Various resources, publications and guides are available to help school district and Board of Cooperative Educational Services (BOCES) (together, "schools") officials develop and implement necessary building access infrastructure and systems to create a safe and secure environment for their students, teachers, staff and visitors.

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 properly manage and monitor building access accounts and key cards.

During our fieldwork in April 2026, the District had 420 active accounts associated with 351 key cards issued to current employees, and 69 key cards issued to non-employees, including 24 shared key cards. We determined:

- 17 individual non-employees had unneeded, duplicate active key cards.
- Nine active shared key cards were never used, and District officials could not locate them.

Non-Employee Accounts – For the 45 individual non-employee accounts, we determined that 17 key cards (38 percent) were unneeded. These 17 active individual non-employee accounts were assigned to local law enforcement agency personnel who no longer used District-issued key cards for building access, instead using their own agency-issued ID cards. Therefore, these 17 key cards, nine of which were never used, were no longer needed and were essentially duplicate key cards.

Additionally, District officials could not locate any of these 17 active key cards. The Middle School Principal (Principal), who additionally functioned as the District's Technology Coordinator, told us that the law enforcement agency informed him that the cards were destroyed. Because neither District officials nor OSC auditors could confirm that the key cards were destroyed, we recommended deactivating the accounts and associated key cards. As a result of our audit inquiry, the Principal deactivated these 17 key cards.

The 24 active shared key cards included nine key cards that were never used and which District officials could not locate. These included six administrator key cards and three key cards for the local fire department. The Principal told us that these were old key cards and that they are not used anymore. As a result of our audit inquiry, the Principal deactivated these nine key cards.

These issues occurred, in part, due to a lack of clear communication of responsibilities, and no documented procedures for managing and monitoring building access, including no regular reconciliation of access accounts and devices using readily available system reports. This increased the risk of unauthorized entry to District school buildings. During our fieldwork, District officials provided us with a copy of a draft policy they prepared that would outline the individuals involved in managing the access system and its key cards, as well as their roles and responsibilities.

Account Management and Monitoring Procedures – The District did not have any written procedures outlining who is responsible for managing and monitoring accounts. Specifically, District officials did not define who is authorized to create accounts, who is responsible for monitoring active accounts, and the process to revoke access by deactivating unneeded accounts and collecting key cards. At the time of our fieldwork, the process for adding, removing, or modifying access accounts was handled by the Principal, who:

- Added accounts for new employees to the system including any access restrictions (e.g., days, times and buildings) based on information about the employee's role and assigned building as specified in an email from the Assistant Superintendent for Management Services (Assistant Superintendent) or Superintendent's Secretary.
- Added accounts for non-employees, including emergency services and contractors.
- Modified access as requested by the Assistant Superintendent, and
- Revoked employee access after notification from the Assistant Superintendent.

The Assistant Superintendent and Principal told us that the Assistant Superintendent was responsible for collecting key cards during the termination meeting held when an employee left District employment and subsequently verbally informing the Principal to deactivate the employee's access account. Additionally, we observed that the system was configured to automatically deactivate accounts after 21 days of inactivity. However, non-employee accounts such as law enforcement, fire safety, and administrative access did not have this setting applied, which contributed to the previously discussed unneeded non-employee accounts with active key cards.

Finally, no one was periodically reviewing active accounts and using available system reports to determine whether all active accounts and key cards were needed and instead relied on the system settings to automatically deactivate accounts. As a result, District officials were unaware that the unneeded law enforcement, fire safety and administrative access accounts were still active. During our fieldwork, we worked with District officials and demonstrated how the system's reports could improve the monitoring and management of building access. When access is not periodically reviewed and revoked, it increases the potential for unauthorized access to District buildings.

Recommendations

District officials should:

1. Deactivate accounts and collect the associated key cards as soon as they are no longer needed.

2. Develop written procedures that define who is responsible for managing and monitoring accounts including shared key cards and periodically evaluate and adjust these procedures to ensure all processes are working as intended.

3. Develop a reconciliation process utilizing system reports and review active accounts for necessity and appropriateness of access.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include portions of the Town of Hempstead in Nassau County. The District's five buildings are located on campuses in the Town of Hempstead.

The District is governed by the elected five-member Board. The Board is responsible for managing and controlling the District's financial and educational affairs. The Superintendent is responsible, along with other administrative staff, for managing the District's day-to-day operations under the Board's direction.

The Superintendent assigned the Principal the responsibility for managing and monitoring accounts. The Principal utilizes the system to set up and issue key cards to users which are then distributed either by him or the IT Aides. The IT Aides have administrative access to the system and can also create, modify and deactivate key cards if the Principal is unavailable to do so.

Criteria

NYSED's Safe Schools by Design Act guidance[2] provides that, as the second line of defense when protecting a building and its occupants, building entry should maintain a welcoming exterior while ensuring safety and security, such as using credentialed electronic access systems. The Cybersecurity and Infrastructure Security Agency's (CISA) K-12 School Security Guide[3] recommends schools should have in place a layered, system-based approach to physical security in which physical security equipment and technology, site and building features, personnel and staff, policies and procedures, and training programs work together to ensure school facilities are secure.

Policies and Procedures – Schools should develop and implement physical security and access control policies and procedures with roles and responsibilities defined and assigned across its organizational entities (e.g., IT, Human Resources, administration, facilities etc.). Policies and procedures should be established to manage, monitor and revoke building access devices and other access credentials as necessary. The policies and procedures should be periodically reviewed and updated to reflect the current and approved access controls implemented within the system and organization.

Building Access/Entry – Schools should control who can enter school buildings, where they can go, and when access is permitted. Building access systems serve as an internal control to help ensure safety and security including controlled entry points, visitor management, and monitoring building access. Internal controls over building access/entry should be designed in a way that primary entrances are controlled through device readers, security desks, or locked-door systems.

Building Access Account Management – Only designated system users/administrators should be able to create, enable, modify, revoke and remove accounts in accordance with documented policies and procedures. System administrators for access management should be limited and have clearly defined roles and responsibilities. Account management processes should align with individual status changes, such as extended leave, termination or other circumstances when access is not required.

Device Issuance and Authorization – Devices should only be issued with documented approval based on job role and building assignment; each device should be unique and individually assigned. Each individual should only have one device. Shared devices should be avoided so that all activity can be logged to a specific individual. When shared devices must be used, a process should be established to track these devices. No

2 https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf
3 https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

individual should be issued a device until a background check is completed, if required. Visitors and contractors should sign in at a single point of entry and receive a visible identification or badge. Contractors' access should be limited to approved locations and timeframes.

Device Management – Devices should be immediately deactivated when no longer necessary. Any necessary updates to building access should happen promptly. Lost or stolen devices should immediately be reported to staff responsible for deactivating devices and replacement devices should be reissued only with documentation approving the reissuance. Device inventory should be tracked, and periodically reconciled and unused or returned devices should be secured or destroyed.

Building Access Event Monitoring – Device events should be logged by user, door and timestamp (i.e., device used at door). These logs should be reviewed periodically and/or upon an unauthorized incident. The building access system should generate alerts for after-hours or unauthorized access attempts if possible. Logs should be retained according to the district policies. Periodically reviewing physical access logs can help identify unexpected activity.

Additional Resources

We also used the following publications to inform our criteria. These publications provide school officials with actionable, practical and cost-effective resources, solutions and tools that enhance school building safety and security:

- **NYSED Safe Schools by Design Act: A Guide by NYSED (April 2025)**
  https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf

- **Partner Alliance for Safer Schools (PASS) Safety and Security Guidelines for K-12 Schools (7th Edition, 2025)**
  https://passk12.org/wp-content/uploads/2025/08/PASS_7thEdition-web.pdf

- **K-12 School Security Guide (3rd Edition, 2022)**
  https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

- **National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations (Revision 5)**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.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, is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[4] and may have included changes to spelling and grammar. The substance of the content was not changed.

MALVERNE UNION FREE SCHOOL DISTRICT
Administrative Offices 301 Wicks Lane
Malverne, New York 11565 516-887-6405
Fax: 516-596-2910

August 20, 2026

Ms. Nicole Tomsen, Chief of Municipal Audits, Statewide Audits
Office of the State Comptroller
Statewide Audit Office
295 Main Street, Suite 1032
Buffalo, New York 14203-2510

Dear Ms. Tomsen,

This correspondence will serve as the official response from the Malverne Union Free School District regarding your draft audit during the period of July 1, 2024-April 21, 2026. Please be assured that the Malverne Board of Education appreciates the efforts of your staff and the recommendations made to further strengthen building access controls. We will carefully consider the recommendations provided by your office in the audit report. The District will prepare and submit a corrective action plan within the required time period and implement corrective actions within an appropriate timeframe.

The District agrees with your recommendations to deactivate accounts and collect associated key cards, develop written procedures that define responsibility for managing and monitoring accounts, and to develop a reconciliation process utilizing system reports and review active accounts for necessity. The District will implement the noted recommendations and continue to provide training to district staff for the safeguarding of building access.

The Malverne Union Free School District wishes to express its gratitude for the Comptroller's assistance and guidance during the audit process, which will benefit the District and its taxpayers. The District looks forward to future opportunities to work with the Comptroller's office.

Sincerely,

Dr. Maria L. Rianna
Superintendent of Schools

CC: Malverne Board of Education

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

Appendix C: Audit Methodology and Standards

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

- We interviewed District officials, reviewed Board policies and the system's settings to gain an understanding of the District's policies, procedures, practices and system access controls related to managing and monitoring accounts and key cards, including roles and responsibilities of the individuals involved in the process.

- We compared the District's 420 active accounts list to the employee master list of employees to determine whether all accounts were associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and key cards assigned to non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

- We selected all 24 non-employee shared accounts and reviewed system reports to determine when assigned key cards were last used. We requested that the Maintenance Supervisor contact the key card holders, including the two law enforcement agencies and the fire department, to determine whether the key cards were in their possession and needed. If the key cards were not in their possession, we suggested that the Principal deactivate the key cards.

- We selected all 45 individual non-employee accounts, reviewed system reports and discussed each account with the Principal to determine when the associated key cards were last used, whether they were accounted for, and whether they were needed.

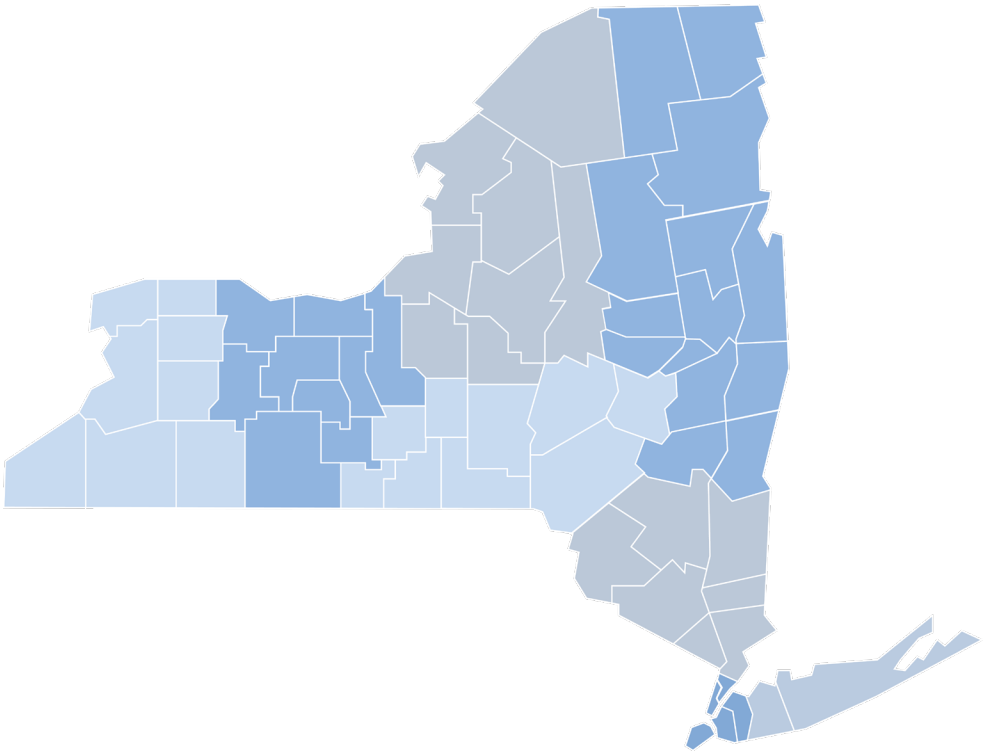
- We reviewed the active accounts list to determine whether any users had more than one account, and why one of the law enforcement agencies had duplicate key cards for their officers.

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.

Questions?

STATEWIDE AUDITS
Nicole A. Tomsen, Chief of Municipal Audits
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • Fax (716) 847-3643
Email: Muni-Statewide@osc.ny.gov



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