

New York State Comptroller
THOMAS P. DiNAPOLI

Brentwood Union Free School District

Building Access

August 2026 | S9-26-12

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results	1
Building Access: Finding and Recommendations	3
Finding 1 – District officials could improve how they manage and monitor building access accounts and badges.	3
Recommendations	4
Appendix A: Profile, Criteria and Resources	5
Profile	5
Criteria	5
Additional Resources	6
Appendix B: Response From District Officials	7
Appendix C: OSC Comment on the District’s Response	9
Appendix D: Audit Methodology and Standards	10

Audit Results

Brentwood Union Free School District

Audit Objective

Did Brentwood 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 14, 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, keycards, 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 2,839 active building access accounts (accounts), including 2,644 devices issued to current employees and 195 issued to non-employees, of which eight are shared badges.¹ Each of the District's 17 school buildings has a single public point of entry. Employees may also access the buildings through additional secured entry points, which require a device for entry. The Safety Office, led by the Director of Safety (Director), was responsible for device management at the District during our audit period.

Audit Summary

District officials could improve how they manage and monitor building access accounts and devices (badges). Although the District had written procedures for building access and badge management that included details regarding the issuance, monitoring and disabling of badges, they were not always followed because the current District practices did not match the written procedures. 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, of the accounts we reviewed, the District had active, but unneeded, accounts with assigned badges in the system:

- Three District employees had duplicate active badges.
- Five non-employee badges were not disabled in a timely manner despite the District's badge management procedures stating officials should disable badges with four months of inactivity.

Although District officials had a process for periodically reviewing active accounts to determine whether they were needed, they did not disable all accounts with inactivity in a timely manner. These issues occurred because District officials did not follow the District's written procedures that clearly described and assigned responsibilities to the Safety Office personnel for managing and monitoring accounts.

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 report includes three recommendations that, if implemented, will help District officials improve management and monitoring of building access accounts and badges. District officials generally agreed with our recommendations and their response is included in Appendix B. Appendix C includes our comment on an issue raised in the District's response.

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the Office of the New York State Comptroller's (OSC's) authority as set forth in Article 3 of the New York State General Municipal Law (GML). The audit's methodology and standards are included in Appendix D.

The Board of Education (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 could improve how they manage and monitor building access accounts and badges.

During our fieldwork in April 2026, the District had 2,839 active accounts associated with 2,644 badges issued to 2,632 current employees, and 195 badges issued to 187 individual non-employees and eight shared badges. We determined:

- Three current employee accounts had duplicate active badges, and
- Five non-employee accounts were not disabled in a timely manner.

Employee Accounts – Three employees had duplicate active badges. We determined that the three duplicate badges were issued as replacements because two original badges were damaged and one original badge had a printing error and was never issued. However, the original badges were not properly disabled. The Director told us Safety Office personnel forgot to disable the original badges when issuing replacement badges. During fieldwork, we verified that the Director properly disabled the three unneeded original badges.

Non-Employee Accounts – We reviewed 19 of the 187 individual non-employee accounts and badges and determined five of these active non-employee badges were not disabled in a timely manner in accordance with the District’s procedures.

According to the District’s badge management procedures, Safety Office personnel should review all badge activity every four months and notify individuals who have not used their badges in the preceding four months to swipe their badge within five school days of notification. Safety Office personnel should disable any remaining badges with inactivity after notification. During our fieldwork in April 2026, Safety Office personnel last performed a review of four-month badge activity on March 25, 2026, when they identified five active individual non-employee badges that were last used between October and November 2025. However, although the five badges were not swiped within five school days of the email notification, Safety Office personnel did not disable the badges.

The Director said these badges were not disabled because the individuals requested Safety Office personnel to not disable their badges. However, the District’s procedures do not state that District officials can extend access based solely on the badge holder’s request. Not adhering to the District’s procedures of disabling badges with four months of inactivity increases the potential risk of unauthorized entry to District school buildings.

Account Management and Monitoring Procedures – District officials established written procedures that clearly defined who is authorized to grant building access accounts, who can be issued a badge and the limits of access (i.e., time or locations necessary for job-related duties), who is responsible for monitoring active accounts, and the process to monitor and revoke access by deactivating unneeded accounts and collecting badges.

The Director told us that the procedures were provided to select Safety Office personnel involved in badge management. However, as discussed earlier in this report, Safety Office personnel did not always follow these procedures, as we identified five badges that should have been disabled due to inactivity. If District officials determine that such a request meets a business need, the request should involve supervisory approval as an additional check, and District officials should update the procedures to reflect this practice. It is important for District employees to adhere to the District's procedures and for District officials to update their procedures to reflect all current practices, because doing so enhances building security and safety for students, teachers, staff and visitors.

Recommendations

District officials should:

1. Ensure employees do not have unneeded duplicate badges.
2. Disable accounts with four months of inactivity and no response from users to notifications to swipe their badge within five school days per the District's written procedures.
3. Consider updating the written procedures that address disabling accounts after four months of inactivity to align with current practices if there is a business need to extend such accounts.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include the Town of Islip in Suffolk County. The District's buildings are located on campuses in the Town of Islip.

The District is governed by the elected seven-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 Safety Office is responsible for managing and monitoring accounts. The Safety Office utilizes the system to print and issue badges directly to users. The Director and select Safety Office personnel have administrative rights to activate, modify and deactivate accounts in the system. The Information Technology (IT) Coordinator and Assistant IT Coordinator also have administrative rights to activate, modify and deactivate accounts in the system if Safety Office personnel are unavailable to do so.

Criteria

NYSED's Safe Schools by Design Act guidance² 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 Guide³ 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 (HR), 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

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. When shared devices must be used, a process should be established to track these devices. No 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's 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-a-guide-by-nysed-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 OSC's 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.

Brentwood Union Free School District
Anthony F. Felicio Administration Building
52 Third Avenue, Brentwood, NY 11717
(631) 434-2325
www.bufsd.org

July 28, 2026

Dear Audit Team:

The Brentwood Union Free School District generally agrees with the audit's recommendations and appreciates the opportunity to further strengthen its existing building access procedures. We also appreciate the professionalism of the audit team throughout the review process.

The District notes that the audit identified eight (8) exceptions within a building access system consisting of 2,839 active accounts and badges. Importantly, the audit did not identify any instances of unauthorized access, misuse of credentials, or security breaches resulting from the exceptions noted [[OSC Comment: See Appendix C, Note 1](#)]. The District believes this distinction is significant, as it demonstrates that the identified issues were administrative in nature rather than failures of the District's overall building security system.

The District is proud of the comprehensive systems, internal controls, and written procedures already in place to safeguard our students, staff, and facilities. We remain committed to continuously reviewing and enhancing these practices to ensure our building access program reflects both sound security practices and the District's operational needs.

The District had established written procedures governing badge issuance, monitoring, and deactivation throughout the audit period. As acknowledged in the report, the duplicate employee badges identified during the audit were replacement badges issued because of damaged cards or a printing error. The original badges were not intentionally maintained as active credentials and were promptly deactivated once they were brought to the District's attention.

With respect to the five inactive employees' badges that remained active beyond the four-month inactivity period, the District acknowledges that these badges were not deactivated in accordance with its written procedures. As discussed during the audit, these individuals continued to have legitimate operational relationships with the District, and Safety Office personnel exercised operational discretion in retaining their access. While the District believes there were valid operational reasons for maintaining these credentials, we agree that such exceptions should be supported by documented supervisory approval and reflected within our written procedures.

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

The District has already begun reviewing and strengthening its building access procedures to ensure that operational practices are consistently documented, monitored, and supported by appropriate supervisory oversight. These efforts include:

- Reinforcing established procedures with Safety Office personnel regarding the immediate deactivation of replacement badges.
- Updating written procedures to establish a formal approval and documentation process when operational needs justify extending badge access beyond the standard inactivity threshold.
- Implementing additional administrative oversight to ensure that badge management decisions are consistently documented and aligned with District procedures.

The Brentwood Union Free School District remains fully committed to maintaining a safe and secure learning environment for our students, staff, and visitors. We value continuous improvement and will incorporate the audit recommendations into our Corrective Action Plan to further enhance our existing practices.

We appreciate the audit team's recommendations and view this review as an opportunity to strengthen an already comprehensive building access system while continuing to ensure the safety and security of our students, staff, and visitors.

Sincerely,

Wanda Ortiz-Rivera
Superintendent of Schools

Appendix C: OSC Comment on the District's Response

Note 1

The audit objective focused on the District's management and monitoring of building access accounts and devices. The audit team assessed the risk of potential security breaches occurring, such as unauthorized access to school buildings, which is significant within the context of this audit objective. Therefore, these audit results cannot be used to conclude there were no security breaches or unauthorized access incidents in the District's operations.

Appendix D: 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 and reviewed Board policies to gain an understanding of the District's policies, procedures and practices related to managing and monitoring building access accounts and badges, including roles and responsibilities of the individuals involved in the process.
- We compared the District's 2,839 active building access accounts list to the master list of employees to determine whether all accounts were associated with current District employees. We also used our professional judgment to select 19 non-employee badge accounts with the oldest date of entry or incomplete details. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and badges assigned to non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We selected all shared badges and inquired with the respective District officials responsible for them to determine whether the badges were necessary and whether they were in their possession.
- We reviewed the active building accounts list to determine whether any users had more than one account and badge and interviewed District officials to determine why users were assigned more than one account. For the three employees with a total of six duplicate badges, we followed up with District employees to determine why individual users had multiple access accounts and badges.

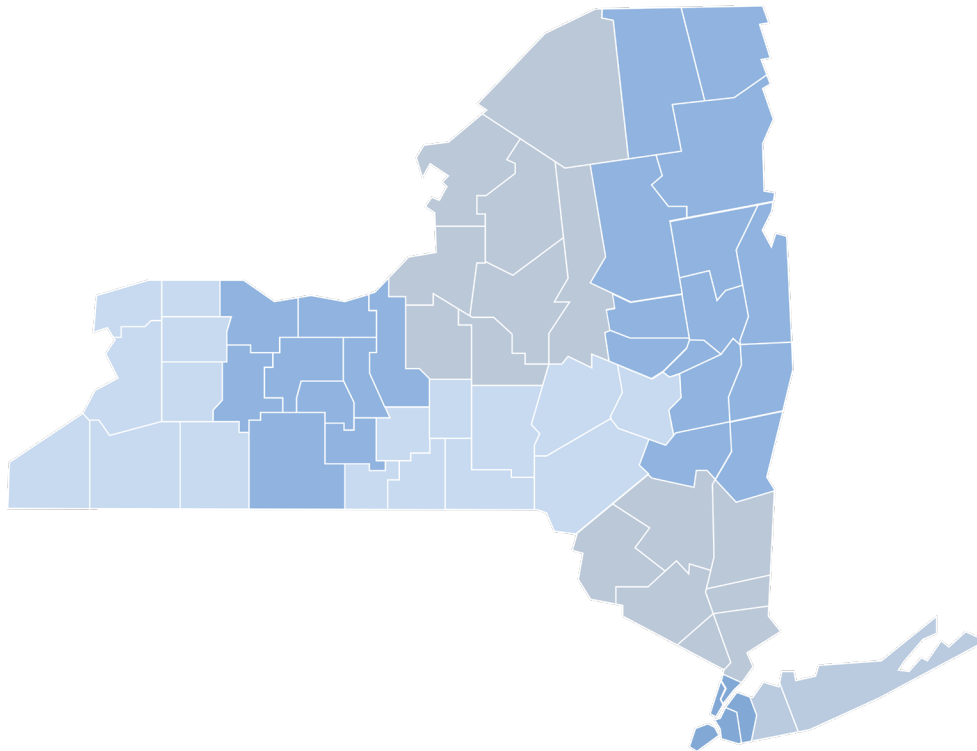
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

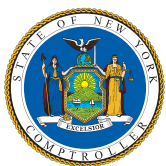
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected 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



FOLLOW US: osc.ny.gov/subscribe