

New York State Comptroller  
THOMAS P. DiNAPOLI

# Holley Central School District

## Building Access

**July 2026 | S9-26-4**

Prepared by the Division of Local Government and School Accountability

# Table of Contents

---

|                                                                                                           |          |
|-----------------------------------------------------------------------------------------------------------|----------|
| <b>Audit Results</b>                                                                                      | <b>1</b> |
| <b>Building Access: Finding and Recommendations</b>                                                       | <b>3</b> |
| Finding 1 – District officials did not properly manage and monitor building access accounts and key fobs. | 3        |
| Recommendations                                                                                           | 4        |
| <b>Appendix A: Profile, Criteria and Resources</b>                                                        | <b>5</b> |
| Profile                                                                                                   | 5        |
| Criteria                                                                                                  | 5        |
| Additional Resources                                                                                      | 6        |
| <b>Appendix B: Response From District Officials</b>                                                       | <b>7</b> |
| <b>Appendix C: Audit Methodology and Standards</b>                                                        | <b>9</b> |

# Audit Results

---

## Holley Central School District

### Audit Objective

Did Holley Central 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 March 12, 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 uses a building access management system (system) with 423 active building access accounts (accounts), including 260 access devices issued to current employees and 163 issued to non-employees, of which 18 are shared access devices.<sup>1</sup> Each of the District's two school buildings has a single public point of entry. Employees and staff 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 fobs). 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 key fobs in the system:

- 14 District employees had two or more key fobs, including the Working Supervisor who was assigned four key fobs.
- 27 non-employee key fobs, including 18 key fobs that were issued to former contractors, were not disabled when no longer needed.

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. Furthermore, these issues occurred because District officials did not establish written procedures that clearly assigned who was responsible for managing and monitoring accounts or develop written policies and procedures for issuing and monitoring key fobs.

---

<sup>1</sup> 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 four recommendations that, if implemented, will help District officials improve management and monitoring of accounts and key fobs. District officials generally agreed with our recommendations and their response is included in Appendix B.

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 C.

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 OSC makes 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 fobs.**

During our fieldwork in March 2026, the District had 423 active accounts associated with 260 key fobs issued to 243 current employees and 163 issued to non-employees, including 145 to individuals and 18 shared key fobs. We determined:

- 6 percent of employee accounts had duplicate active key fobs, and
- 17 percent of non-employee accounts were unneeded.

Employee Accounts – Of the 243 employees, 14 employees (6 percent) were assigned two or more active key fobs, including one employee with four active key fobs. The Director of Facilities (Director) told us that duplicate key fobs were issued for the convenience of 12 employees, including teachers, clerical staff and custodians, though their job duties did not require multiple key fobs. In addition, the Director and the Working Supervisor retained three and four active key fobs, respectively, which they believed was necessary as a backup in case of emergency.

When we brought these issues to District officials’ attention, the Director told us that the District deactivated a total of 15 key fobs, including one associated with the Director, two associated with the Working Supervisor, and 12 associated with other employees. However, the Director and the Working Supervisor each still retained two active key fobs, though both officials have an alternative method (physical key) to enter any exterior door on any of the buildings without the need for a key fob. Allowing employees to retain multiple active key fobs increases the risk of lost or stolen key fobs and unauthorized entry to District school buildings.

Non-Employee Accounts – Of the 145 individual non-employee key fobs, we identified and reviewed with District officials 86 accounts whose purposes needed further clarification.<sup>2</sup> Of the 86 accounts, a total of 27 accounts (17 percent) were no longer needed:

- 18 were issued to former contractors that no longer provided services to the District,
- Five were used for building access testing but were no longer needed, and
- Four were issued to former employees.

After our audit inquiry, District officials disabled these 27 accounts and associated key fobs. The remaining 59 accounts we reviewed were appropriately assigned to individuals who required access for District business purposes.

The 18 active shared key fobs were used for substitute employees, such as teachers and custodians. Officials told us that designated department heads, such as facilities, had custody of these key fobs when they were not

---

<sup>2</sup> See Appendix C for details of our testing methodology.

in use. However, officials did not maintain a written log or any other record to track who used these key fobs, diminishing accountability and limiting officials' ability to detect loss or potential misuse. When we brought these issues to District officials' attention, the Director deactivated 15 shared key fobs.

Because the District did not have written procedures for staff to follow or a periodic reconciliation of access, there is a risk that shared key fobs were not collected. Additionally, there were no procedures for the supervisors of the substitute employees to track or collect shared key fobs each day.

Account Management and Monitoring Procedures – District officials did not assign roles and responsibilities for all parties involved in the building access management process or have any written procedures outlining who is responsible for managing and monitoring accounts, including who is authorized to create accounts, who is responsible for monitoring active key fobs, and the process to revoke access, by deactivating unneeded accounts and collecting key fobs. At the time of our audit in March 2026, the Director was solely responsible for:

- Adding accounts for new employees to the system, including any access restrictions (e.g., time or a specific entry point) based on the employee's role and required access.
- Issuing prenumbered key fobs to employees.
- Reissuing key fobs if necessary (e.g., lost or damaged key fobs).

Additionally, the Director told us he monitored active key fobs and was responsible for lost device deactivation, as well as collecting, deactivating and destroying key fobs that were no longer needed due to resignation, retirement or termination.

The Director and Working Supervisor had the same administrative rights in the system to make modifications including activating, deactivating or modifying building access. During our audit period, the Director and Working Supervisor both made updates and changes to access accounts. However, the Director told us that the Working Supervisor would not make any changes unless the Director told him to do so. Additionally, no one was periodically reviewing active accounts to determine whether all active accounts were needed. As a result, account updates were not always made in a timely manner and there was a potential for unauthorized access to District buildings.

## Recommendations

District officials should:

1. Deactivate accounts and collect the associated key fobs as soon as they are no longer needed.
2. Ensure employees do not have duplicate key fobs.
3. Develop written procedures that define who is responsible for managing and monitoring accounts including shared key fobs and periodically evaluate and adjust these procedures to ensure all processes are working as intended.
4. 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 the Towns of Albion, Barre, Clarendon and Murray in Orleans County and the Town of Clarkson in Monroe County. The District's buildings are located on campuses in the Town of Murray.

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 Superintendent assigned the Director the responsibility for managing and monitoring building access accounts. The Director utilizes the system to issue key fobs to users which are distributed either by him or department heads. The Working Supervisor also has administrative rights to activate, modify and deactivate accounts in the system if the Director is unavailable to do so.

## Criteria

NYSED's Safe Schools by Design Act guidance<sup>3</sup> 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<sup>4</sup> 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 individual. When shared devices must be used, a process should be established to track these devices. No

---

<sup>3</sup> <https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf>

<sup>4</sup> <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 (7<sup>th</sup> Edition, 2025)**  
[https://passk12.org/wp-content/uploads/2025/08/PASS\\_7thEdition-web.pdf](https://passk12.org/wp-content/uploads/2025/08/PASS_7thEdition-web.pdf)
- **K-12 School Security Guide (3<sup>rd</sup> 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)*,<sup>5</sup> and may have included changes to spelling and grammar. The substance of the content was not changed.

HOLLEY CENTRAL SCHOOL DISTRICT  
3800 North Main Street  
Holley, NY 14470  
Phone (585) 638-6316 | Fax (585) 638-7409  
[www.holleycsd.org](http://www.holleycsd.org)

July 20, 2026

Nicole A. Tomsen, Chief of Municipal Audits  
Division of Local Government and School Accountability  
110 State Street  
Albany, NY 12236

Re: Response to Draft Audit Report - Building Access Controls S9-26-4

Dear Ms. Tomsen,

We are grateful for the professionalism of the audit team and for the thoughtful feedback provided. This process has been valuable in helping us strengthen our systems and further align our practices with our commitment to maintaining a safe, supportive, and well-managed learning environment for students, staff, and visitors. We view this as an important opportunity to improve our procedures and internal controls.

The District acknowledges the finding regarding the need to strengthen management and monitoring of building access accounts and key fobs. We have already taken, and will continue to take, proactive steps to address each of the four recommendations outlined in the report.

1. Deactivate accounts and collect associated key fobs when no longer needed.

The District has taken immediate action to deactivate unnecessary accounts and associated key fobs identified during the audit process. This includes deactivation of duplicate and inactive fobs, particularly those assigned to former contractors and individuals no longer requiring access. Going forward, access will be promptly deactivated upon separation of employment or completion of contracted services, and procedures will ensure timely collection of issued devices. This work strengthens our ability to consistently safeguard our facilities and the people within them.

2. Ensure employees do not have duplicate key fobs.

The District has reviewed all employee access assignments and has eliminated duplicate key fobs where not operationally necessary. Remaining assignments are aligned to job responsibilities, with a clear expectation of one device per individual unless a documented exception is approved. Additional monitoring protocols have been implemented to prevent the reoccurrence of duplicate issuance, reinforcing clear expectations and accountability across roles.

3. Develop written procedures defining roles and responsibilities for managing and monitoring access.

---

<sup>5</sup> <https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule>

The District has developed and implemented a formal, written procedural document outlining the processes for activating and deactivating access fobs. This document clearly defines roles and responsibilities, including authorization, issuance, tracking, and revocation of access. It also includes expectations for management of shared devices and establishes accountability at each step of the process. These procedures support consistency in practice and ensure that staff members have clear guidance in carrying out their responsibilities.

4. Develop a reconciliation process and periodically review active accounts.

The District has established a formal reconciliation protocol utilizing system-generated reports to regularly review active accounts for necessity and appropriateness. In addition, the District will conduct three internal audits (September, January and June) annually to systematically review building access controls, verify alignment with procedures, and ensure that all accounts remain appropriate and necessary. This ongoing review process reflects our commitment to continuous improvement and responsible stewardship of district resources.

The District remains fully committed to maintaining strong internal controls and prioritizing safety across all of our facilities. These improvements are part of our broader effort to create environments where students can learn, staff can work effectively, and all individuals feel secure and supported. Strengthening our systems in this way reinforces the trust placed in us by our community and supports consistent, reliable practices across the organization.

We appreciate the collaborative nature of this process and the guidance provided in strengthening our practices. The District will continue to monitor implementation closely and ensure sustained adherence to established procedures.

Thank you again for the opportunity to respond and to improve our systems and processes.

Respectfully,

Karri D. Schiavone  
Superintendent  
Holley Central School District

# 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 and reviewed Board policies to gain an understanding of the District's policies, procedures and practices related to managing and monitoring accounts and key fobs, including roles and responsibilities of the individuals involved in the process.
- We compared the District's 423 active key fobs list to the employee master list of employees to determine whether key fobs existed that were not associated with current District employees. We identified 163 active key fobs that were issued to non-employees and inquired with the District officials for identification and purpose of 86 of the 163 key fobs, based on the names that were associated with the accounts. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and key fobs assigned to non-employees were necessary. For any unnecessary key fobs, we inquired as to why they were not deactivated.
- We identified 18 shared key fobs and inquired with the respective District officials responsible for the associated key fobs to determine their purpose, whether they were in their possession, and whether the officials maintained a written log to track usage of these key fobs.
- We reviewed the active key fobs list to determine whether any individuals had more than one device and identified 14 employees who were assigned a total of 31 duplicate key fobs. We interviewed the Director and reviewed the last access information to determine why these employees were assigned more than one access device.

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 the findings and conclusions based on the audit objective. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

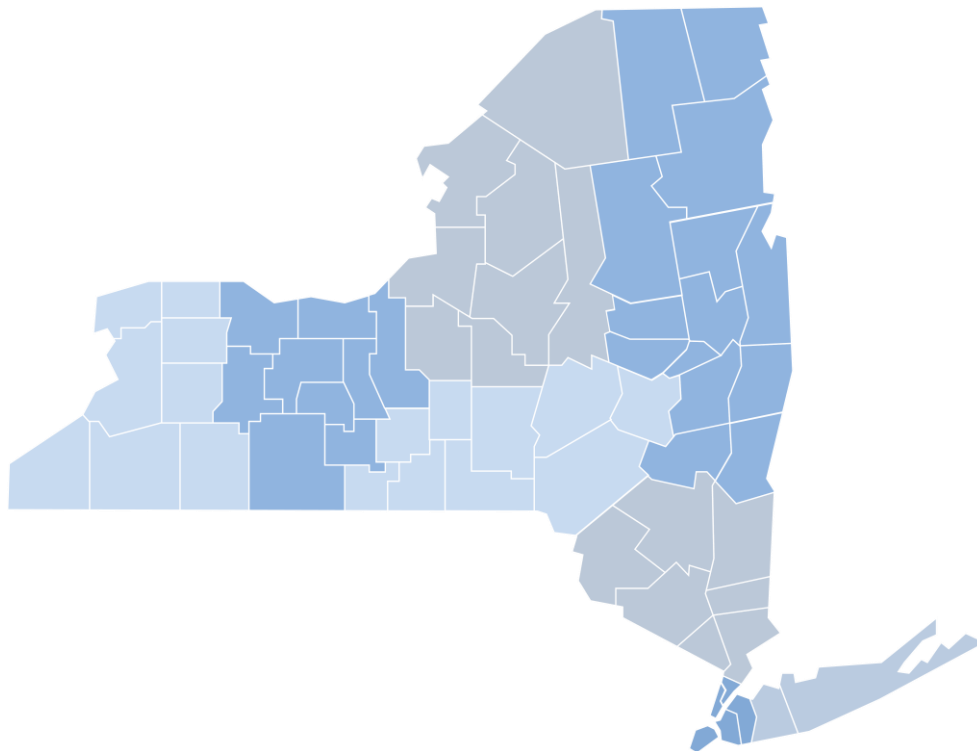
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected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

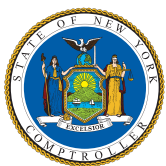
# Questions?

---

## 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](mailto: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](http://www.osc.ny.gov)

Prepared by the Division of Local Government and School Accountability



FOLLOW US: [osc.ny.gov/subscribe](http://osc.ny.gov/subscribe)