



Wayland-Cohocton Central School District

Building Access Accounts and Badges

2024M-113 | December 2024

Contents

- Report Highlights 1**

- Building Access Accounts and Badges 2**
 - How Should District Officials Manage and Monitor Building Access Accounts and Badges? 2
 - Officials Did Not Adequately Manage and Monitor Building Access Accounts and Badges 3
 - What Do We Recommend? 5

- Appendix A – Response From District Officials 6**

- Appendix B – Audit Methodology and Standards 8**

- Appendix C – Resources and Services 10**

Report Highlights

Wayland-Cohocton Central School District

Audit Objective

Determine whether Wayland-Cohocton Central School District (District) officials properly managed and monitored building access accounts and badges.

Key Findings

District officials did not properly manage and monitor building access accounts and badges used to access District buildings. Accounts and badges that are not properly managed and remain active can potentially result in unauthorized building access. District officials:

- Did not establish written procedures that define who is responsible for managing and monitoring building access accounts. Although we determined that the District had a process for granting access and adding information into the Building Access System (BAS) for employees during the hiring process, including background checks, the District did not have an adequate process for granting access to non-employees. Almost half of the active building access accounts and badges were for non-employees.
- Did not establish a Service Level Agreement (SLA) with the third-party contractor that issued and managed 209 building access accounts and badges.
- Granted access to 39 individuals participating in continuing education programs without conducting any background checks.
- Issued 14 building access accounts and badges without verification from District administrators that these individuals were approved to receive access.
- Did not deactivate the building access account of, and could not locate the badge for, one non-employee. The account and badge were no longer needed as of December 1, 2023 but still active as of July 15, 2024.

Recommendations

The audit report includes six recommendations to help the Board and District officials improve the management and monitoring of building badge access accounts and badges. District officials generally agreed with our recommendations and indicated they will take corrective action.

Audit Period

July 1, 2023 – June 30, 2024

Background

The District serves the Towns of Conesus, Sparta and Springwater in Livingston County, the Towns of Canadice and Naples in Ontario County, and the Towns of Avoca, Cohocton, Dansville, Fremont, Prattsburgh and Wayland in Steuben County.

The District is governed by an elected seven-member Board of Education (Board). The Board is responsible for managing and controlling the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is responsible, along with other administrative staff, for managing the District's day-to-day operations under the Board's direction.

The Information Technology Coordinator (IT Coordinator) and Audio-Visual Coordinator (AV Coordinator) are responsible for managing and monitoring the use of building access accounts and badges. The District uses a third-party security system provider to manage and monitor first responder building access accounts and badges.

Quick Facts

Active Building Access Accounts	
Employees and Board Members	335
Non-Employee Individuals	76
Generic Shared Accounts	243
Total	654

Building Access Accounts and Badges

The District has implemented a BAS that assists officials to manage and monitor building entry points and regulates who can enter the school premises. This system uses ID badges, with building access accounts stored in the computer program which authenticates the approved badge holder before allowing entry to District buildings.



How Should District Officials Manage and Monitor Building Access Accounts and Badges?

The Safe Schools Against Violence in Education Act (SAVE Act)¹ requires school district (district) officials to incorporate school building security into their safety plans, including the implementation of physical security devices, such as badges that allow access to buildings. Officials should also establish written procedures for managing employee and non-employee badge accounts that define:

- Who at the district has the authority to grant access,
- To whom access and badges can be issued and the limits of access (i.e., time period or locations necessary for job-related duties),
- Who is responsible for monitoring active accounts, and
- The process to revoke access, by collecting and deactivating accounts and badges.

District officials should also periodically review all building access accounts to help monitor and ensure that any account not associated with an authorized user, or a current need is promptly deactivated. To ensure individual accountability, all employees should have and use their unique building access accounts and badges to access district buildings. For building access accounts and badges not assigned to a specific individual, officials may not be able to link activity directly to an individual. If shared building access accounts and badges are necessary, officials should establish additional procedures to track and monitor account usage and ensure badges are collected after use. When shared building access accounts and badges are not needed, they should be deactivated. Badges that remain active for building access accounts without a purpose can be lost, stolen or misused, potentially leading to unauthorized building access.

In addition, district officials should have a separate written SLA between the district and its security system provider that identifies the district's needs and expectations and specifies the level of service to be provided for the building access. An SLA provides detailed explanations of the services to be performed by identifying:

- The parties and defining terminology,
- Term or duration of the agreement,
- Scope and/or subject limitations,
- Service level objectives,
- Performance indicators,
- Roles and responsibilities,
- Nonperformance impact,
- Security and audit procedures,
- Reporting requirements,
- Review, update and approval processes, and
- Scope of services to be provided.

¹ An act to amend New York State Education Law, in relation to improving school safety (Laws of New York, 2000, Chapter 181).

Officials Did Not Adequately Manage and Monitor Building Access Accounts and Badges

The District did not establish written procedures that define who is authorized to grant building access accounts, who can be issued a badge and the limits of access (i.e., time period or locations necessary for job-related duties), who is responsible for monitoring active accounts, and the process to revoke access, by deactivating accounts and collecting badges. Without a clear definition or description of roles and responsibilities, District officials cannot ensure that building access accounts and badges are properly issued, managed and monitored.

In the absence of such written procedures, the District's IT Coordinator or AV Coordinator were tasked with adding new building access accounts and badges for employees and non-employees to the BAS, updating access rights, monitoring usage and deactivating accounts and badges. The District had a process for granting building access for employees during the hiring process, including background checks. However, officials did not have an adequate process for granting access to non-employees. Specifically, officials did not perform background checks on individuals participating in continuing education programs or require outside contractors to complete any application, before a District administrator, such as a department head or other designated official, authorized badge access.

We compared all 654 active badge access accounts in the BAS with the current District employee master list and Board member list and identified 335 accounts that were assigned to current employees or Board members. Of the remaining 319 accounts, 76 were assigned to an individual and 243 were not assigned to an individual and are considered generic shared badge access accounts.

Individual Building Access Accounts and Badges – We reviewed 20 active accounts that were assigned to employees and determined that they were necessary based on the employees' job duties. However, we identified that one of the 76 active building access accounts issued to non-employee individuals was not needed and officials should have deactivated the account and collected the badge. This active account was associated with a former employee who resigned December 1, 2023. The AV Coordinator told us the former employee was on extended leave and did not return to their position. The AV Coordinator was unsure why the account was not deactivated and the badge was not collected as the former employee's other computer access was disabled. The badge access account was deactivated on July 15, 2024 when we brought it to officials' attention and the former employee was contacted to return the badge.



We reviewed 15 of the remaining 75 active building access accounts issued to non-employee individuals and determined that 14 of these individuals were issued accounts and badges without the IT Coordinator or AV Coordinator verifying that they were approved by a District administrator or designated official. Also, the District did not require any authorization forms that detail the limits of access, such as time period and locations necessary for job-related duties for outside contractors.

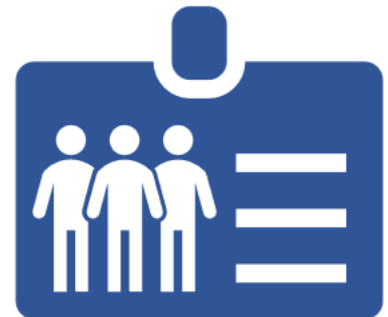
In addition, 39 non-employee individuals participating in continuing education programs received building access accounts and badges without undergoing any background check. Intended for community members at large, the continuing education programs allow participants to access the

District facilities for various activities, such as walking and swimming, with access limited to a specified timeframe before and after school hours. However, it is vital that the District ensures a safe environment is provided to students and staff.

Furthermore, the District has existing technology² which is used to check incoming visitors into District buildings quickly and provides some assurances that visitors do not appear on any registry that should prevent their access. District officials have not leveraged this technology to ensure non-employees with building access accounts should have badge access to District buildings. As part of our audit testing, we checked all 39 individuals against the New York State Division of Criminal Justice Services' sex offender registry and did not find any of the continuing education program participants listed on the registry.

The IT Coordinator told us they receive notification from various District administrators to provide access to District buildings for outside contractors without any information detailing the building location(s) or specific time periods the access is needed. In addition, the Continuing Education Coordinator verbally informs the IT Coordinator that an individual's continuing education program application has been approved and requests the building access without the IT Coordinator knowing whether the individual has been properly vetted and authorized. The Continuing Education Coordinator told us she does not conduct any vetting of individuals by completing a background check. Without an adequate process to verify and authorize access to the District facilities for non-employees, the District cannot ensure the safety of students and employees.

Generic Shared Building Access Accounts and Badges – Of the 243 identified shared building access accounts and badges that were issued, 34 were for substitute personnel and the remaining 209 were provided to first responders. We selected all substitute building access accounts and followed up with the respective departments to verify whether the badges for those accounts were in their possession. One shared building access account established for use at the elementary school was not properly managed because the account's badge could not be located.



The Principal of the elementary school told us they were unaware of the location of the badge, as it was the former secretary's responsibility to receive each badge being used daily. However, the badge went unnoticed until we brought it to the attention of the IT Coordinator who deactivated the badge's associated building access account on August 7, 2024. The badge was last used on July 30, 2024. The AV Coordinator told us that the individual who had the badge changed positions and should have received an individual building access account and badge instead of the continued use of the shared badge.

² The visitor system scans a visitor's driver's license and confirms the visitor and identification match, and that the visitor is not registered in any sex offender database for all U.S. states and territories. The process takes less than two minutes.

The 209 shared building access accounts and badges for first responders are managed and monitored by a third-party security system provider. The Superintendent told us the provided services are part of an informal cooperative agreement between the security system provider, first responders and school districts within Steuben County. However, the District does not have a written SLA with the security system provider that identifies the District's needs and expectations, specifies the level of service to be provided, or identifies who should be allowed access to the BAS to create, modify and deactivate building access accounts and badges and determine when a periodic review of the badge accounts will be completed and reported to the District.

The AV Coordinator told us that they periodically monitored for any suspicious badge activities, dormant building access accounts and badge activity for employee and non-employee building access accounts. However, unneeded individual and shared building access accounts and badges remained active in the BAS because District officials did not adequately review accounts for necessity.

What Do We Recommend?

District officials should:

1. Develop written procedures that define who is responsible for managing and monitoring building access accounts and badges, and evaluate and adjust these procedures, as needed, to ensure all processes are working as intended.
2. Deactivate building access accounts and collect the associated badges as soon as they are no longer needed.
3. Develop a periodic review process, and periodically review active building access accounts for necessity and appropriateness of access.
4. Consider performing background checks for non-employee individuals who participate in continuing education programs prior to authorizing their building access account and badge for access to District buildings.
5. Ensure department heads are aware of the procedures in place for generic shared building access accounts and badges and to monitor who uses them and when and how they are used.

The Board and District officials should:

6. Develop an SLA with the District's third-party security system provider. Ensure the agreement defines the mutual understanding of the District's needs and expectations and specifies the provider's roles and responsibilities.

Appendix A: Response From District Officials

WAYLAND-COHOCTON CENTRAL SCHOOL

Jennifer A. Billotte High School Principal
 Wendi L. Snyder Middle School Principal
 Theresa A. Carhart Elementary School Principal
 Cindy A. Flowers Director of Business, Finance & Facilities
 Rebecca L. Wager Director of Curriculum & Instruction
 Katherine A. Wolcott Director of Pupil Personnel & Special Services

Rich Rizzieri
 President, Board of Education

Eileen M. Feinman Ed.D.
 Superintendent

Superintendent's Office
 213-4303

Business Office
 728-2212

Bus Garage
 728-2213

Counseling Office
 728-2214

Curriculum & Instruction Office
 728-2211

CSE/CPSE Office
 728-9547

High School Office
 728-2366

High School Nurse
 728-2796

Middle School Office
 728-2551

Middle School Nurse
 728-3006

Elementary Office
 728-3547

Elementary Nurse
 728-2091

Prekindergarten Office
 384-5234

December 11, 2024

To Whom It May Concern:

We would like to extend our sincere gratitude to the Office of the NY State Comptroller for their valuable insights and recommendations. Ensuring the safety of our students, staff, and community members remains our highest priority, and we deeply appreciate the guidance provided in this audit. We view the audit findings as effective management tools in improving our Building Access Accounts and Badges process.

We appreciate the opportunity to respond to the draft audit findings and recommendations. The district acknowledges the areas identified for improvement and offers the following response to the specific findings outlined in the draft audit report.

Key Finding 1:

- District officials did not establish written procedures that define who is responsible for managing and monitoring building access accounts. Although we determined that the District had a process for granting access and adding information into the Building Access System (BAS) for employees during the hiring process, including background checks, the District did not have an adequate process for granting access to non-employees. Almost half of the active building access accounts and badges were for nonemployees

The district generally agrees with the finding that officials did not properly manage and monitor building access accounts and badges. The district has an established process for granting access and adding information into the Building Access System (BAS) for employees during the hiring process, which includes background checks. While we agree with the findings regarding employee access management, the district disagrees with the assertion that an inadequate process exists for granting access to non-employees.

It is important to note that although 209 of these badges are assigned to non-employees; all of those individuals are emergency response officers, who require 24/7 access to ensure swift responses during emergencies.

Key Finding 2:

- District officials did not establish a Service Level Agreement (SLA) with the third-party contractor that issued and managed 209 building access accounts and badges.

While the district agrees that a formal Service Level Agreement (SLA) with the third-party contractor managing and accessing these accounts was not established, a contract is already in place with this vendor under the district's Capital Improvement Projects. Moving forward, the district will work with the vendor to formalize an SLA to enhance oversight and clarity of responsibilities.

2350 Route 63, Wayland, NY 14572-9404
 Fax: (585) 728-3566
www.wccsk12.org

WAYLAND-COHOCTON CENTRAL SCHOOL

Jennifer A. Billotte High School Principal
Wendi L. Snyder Middle School Principal
Theresa A. Carhart Elementary School Principal
Cindy A. Flowers Director of Business, Finance & Facilities
Rebecca L. Wager Director of Curriculum & Instruction
Katherine A. Wolcott Director of Pupil Personnel & Special Services

Key Finding 3:

- District officials granted access to 39 individuals participating in continuing education programs without conducting any background checks.

The district acknowledges that access was granted to 39 individuals participating in continuing education programs without background checks. However, as a community-centered district, the campus also serves as a hub for activities such as hall walking and swimming. The 39 community members were all well-known to staff, however, we have strengthened procedures to enhance security by requiring all participants to be screened through the [redacted] before receiving access. Additionally, hall walkers are now issued identifiable badges, and all hall passes will expire and be deactivated on June 30 of each school year.

Key Finding 4:

- District officials issued 14 building access accounts and badges without verification from District administrators that these individuals were approved to receive access.

The district acknowledges that access was granted to 14 individuals through verbal approval but not with written documentation of permission. The 14 individuals were either contractors or worked in partnership with the District through the Center for Youth or Pro-Action.

- District officials did not deactivate the building access account of, and could not locate the badge for, one nonemployee. The account and badge were no longer needed as of December 1, 2023 but still active as of July 15, 2024.

Regarding the finding that a building access account and badge for one non-employee were not deactivated in a timely manner, the district agrees with this observation. This instance involved an employee who resigned while on maternity leave. The employee was hired on 9/05/23, on 11/13/23 she was approved for maternity leave and resigned on 12/01/23. The badge was located during the audit, and it was confirmed that it was never utilized after issuance. Nevertheless, the district has taken steps to ensure that similar oversights do not occur in the future by implementing stricter protocols for deactivating access for employees and non-employees whose accounts are no longer required.

The district is committed to continuously improving its procedures to ensure security, accountability, and compliance. We will carefully review all recommendations and incorporate them into a comprehensive corrective action plan.

Thank you for your efforts in identifying areas where the district can improve its operations and security measures.

Respectfully,

Eileen M. Feinman, Ed.D
Superintendent
Wayland-Cohocton Central School District

2350 Route 63, Wayland, NY 14572-9404
Fax: (585) 728-3566
www.wccsk12.org

Appendix B: Audit Methodology and Standards

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

- We interviewed District officials and reviewed Board policies to gain an understanding of the District's policies, procedures and practices related to managing and monitoring access for District buildings.
- We compared the District's active building access account list to the employee master list and Board member list and identified accounts that were not associated with current District employees or Board members. To determine whether the District needed building access accounts and badges assigned to non-employee individuals, we interviewed District officials and reviewed relevant documentation. For any unneeded building access accounts, we inquired as to why they were not deactivated and identified when the individual separated service from the District and the last time the account was used.
- We judgmentally selected 20 employees and 15 non-employees, consisting of five individuals in adult programs, five individuals working in youth programs and five outside contractors, to determine whether building access accounts assigned were authorized, building access was appropriate and whether building access accounts were needed.
- We selected all building access accounts designated for substitutes and followed up with the respective department heads to verify whether the physical badges for the associated accounts were in their possession. If not in their possession, we inquired as to the reasons why. We also reviewed the badges' activity in the BAS to identify when the badges were last used.
- We reviewed the building access account list and identified the individuals who had more than one badge assigned to the account. We then interviewed District officials to determine why.

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 size of the relevant population and the sample selected for examination.

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 General Municipal Law, Section 2116-a (3)(c) of 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 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.

Appendix C: Resources and Services

Regional Office Directory

www.osc.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas

www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems

www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders

www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller

www.osc.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers

www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics

www.osc.ny.gov/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

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

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

STATEWIDE AUDITS – Dina M.L. Thompson, Chief of Municipal Audits

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Statewide@osc.ny.gov

[osc.ny.gov](https://www.osc.ny.gov)

