DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-156

Greenville Central School District

Network User Accounts

MAY 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Greenville Central School District

Audit Objective

Determine whether Greenville Central School District (District) officials established adequate network user account controls to prevent unauthorized use or access.

Key Findings

District officials did not establish adequate policies and procedures for network user accounts to prevent unauthorized use or access. Officials did not:

- Develop a comprehensive acceptable use policy (AUP) and monitor employee computer use.
- Disable 64 unneeded network user accounts, which included generic and former student and employee accounts.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Ensure the acceptable use policy clearly states what is acceptable for District computer use, is updated to include District employees and is regularly reviewed and monitored for compliance.
- Design and implement procedures to monitor employees' computer use and implement procedures to ensure compliance with the policy.
- Periodically review user access and disable user accounts no longer needed.

District officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The District serves the Towns of Berne, Coeymans, New Scotland, Rennselaerville and Westerlo in Albany County; Cairo, Coxsackie, Durham, Greenville and New Baltimore in Greene County; and Conesville in Schoharie County.

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

The Superintendent of Schools (Superintendent) is appointed by the Board. He is the District's chief executive officer and is responsible for the day-to-day management under the Board's direction.

The District's Director of Technology (IT Director) is responsible for monitoring network user accounts.

Quick Facts	
Network User Accounts	765
Employees	273
Students	1,118

Audit Period

July 1, 2019 – February 8, 2021. We extended our scope period forward to March 31, 2021 to complete computer testing.

Network User Accounts

How Should District Officials Manage Network User Accounts?

Network user accounts provide access to network resources and should be actively managed to minimize the risk of misuse. Therefore, school districts should have written procedures for granting, changing and disabling user accounts.

Officials should disable unnecessary accounts as soon as there is no longer a need for them. In addition, to minimize the risk of unauthorized access, school district officials should maintain a list of authorized user accounts and regularly review enabled network user accounts to ensure they are still needed.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Officials should routinely evaluate generic network user accounts and disable those that are not related to a specific need.

Officials Did Not Adequately Manage Network User Accounts

The IT Director was responsible for ensuring that the District's network user accounts were managed in a timely and satisfactory manner. Although District officials had a procedure in place to add and remove user accounts, we found that the IT Director did not follow the procedure for managing user accounts that were assigned to former employees and students and for unneeded generic accounts. In addition, he did not maintain a list of authorized users or regularly review enabled network user accounts to ensure they were still needed.

We reviewed all 190 user accounts that had not been used in at least six months to determine whether they were still needed. We found that 27 of the 190 user accounts belonged to former employees or students that should have been disabled. We also reviewed all 68 generic accounts and found that 37 (54 percent) were no longer needed. However, the IT Director did not disable the user accounts that belonged to the former employees or students or the unneeded generic accounts.

The IT Director told us he typically did not monitor user accounts unless there was a change in an employee's position, or the Superintendent asked him to permit or restrict access for a specific user account. Therefore, he did not monitor generic accounts.

If not properly managed, network user accounts could provide potential entry points into the District's network that attackers could use to inappropriately access and view personal, private and sensitive information (PPSI).[1]

Why Should the District Establish an Acceptable Use Policy?

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. School district officials can reduce the risks to PPSI and IT assets by adopting an AUP, limiting personal or other Internet use and monitoring usage.

School district officials should develop effective guidelines for network users. School districts should have an AUP that defines the procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources, the school district board's expectations concerning personal use of IT equipment and consequences for violating the AUP.

District officials should develop procedures for monitoring compliance with the District's AUP. Procedures should include routinely monitoring Internet usage and requiring web filtering software to block access to unacceptable websites and limit access to sites that do not comply with the District's AUP.

Officials Did Not Develop a Comprehensive Acceptable Use Policy or Monitor Computer Use

The District's acceptable use policy defined the terms for computer, Internet, and email use only for students. Although the policy does not include guidelines for District employees Internet use, the IT Director told us that all District employees are expected to follow the policy as well.

The AUP states that email usage should be limited to District purposes. Although the policy describes what constitutes prohibited use of IT resources, it does not describe appropriate usage or address acceptable personal use, such as personal shopping and online banking, and/ or accessing personal social media and travel websites.

Officials and direct supervisors did not monitor employee Internet use or implement procedures to monitor for personal Internet use.

[1] PPSI is any information to which unauthorized access, disclosure modification, destruction or use or disruption of access or use could have or cause a severe impact on critical functions, employees, customers, third-parties or other individual or entities.

We examined the web browsing history of five computers[2] used by five employees, whose job duties routinely involved accessing PPSI, to determine whether the employees used the computers for nonbusiness purposes. We found evidence of personal use on all five computers.[3]

The IT Director told us all Internet usage was logged and filtered by a set of rules. The filter rules for faculty and staff were less stringent than those for students. The IT Director also told us that officials did not actively monitor individual Internet usage for compliance with the AUP unless they had a reason to investigate Internet usage or history.

When employees access websites for nonbusiness purposes, productivity is reduced. Also, the District has an increased risk that IT assets and user information could be compromised through malware.

What Do We Recommend?

District officials should:

1. Immediately disable the 27 user accounts belonging to former employees or students and the unneeded 37 generic accounts that are identified in this report. Going forward, periodically review user access for all network user accounts and disable user accounts when access is no longer needed.

2. Ensure the AUP clearly states what is acceptable for District computer use, is updated to include District employees and is regularly reviewed.

3. Design and implement procedures to monitor employees' computer use and implement procedures to ensure that employees comply with the AUP.

[2] Refer to Appendix C for further information on our sample selection.

[3] Refer to Figure 1 in Appendix A for detailed information related to employees' personal Internet use.

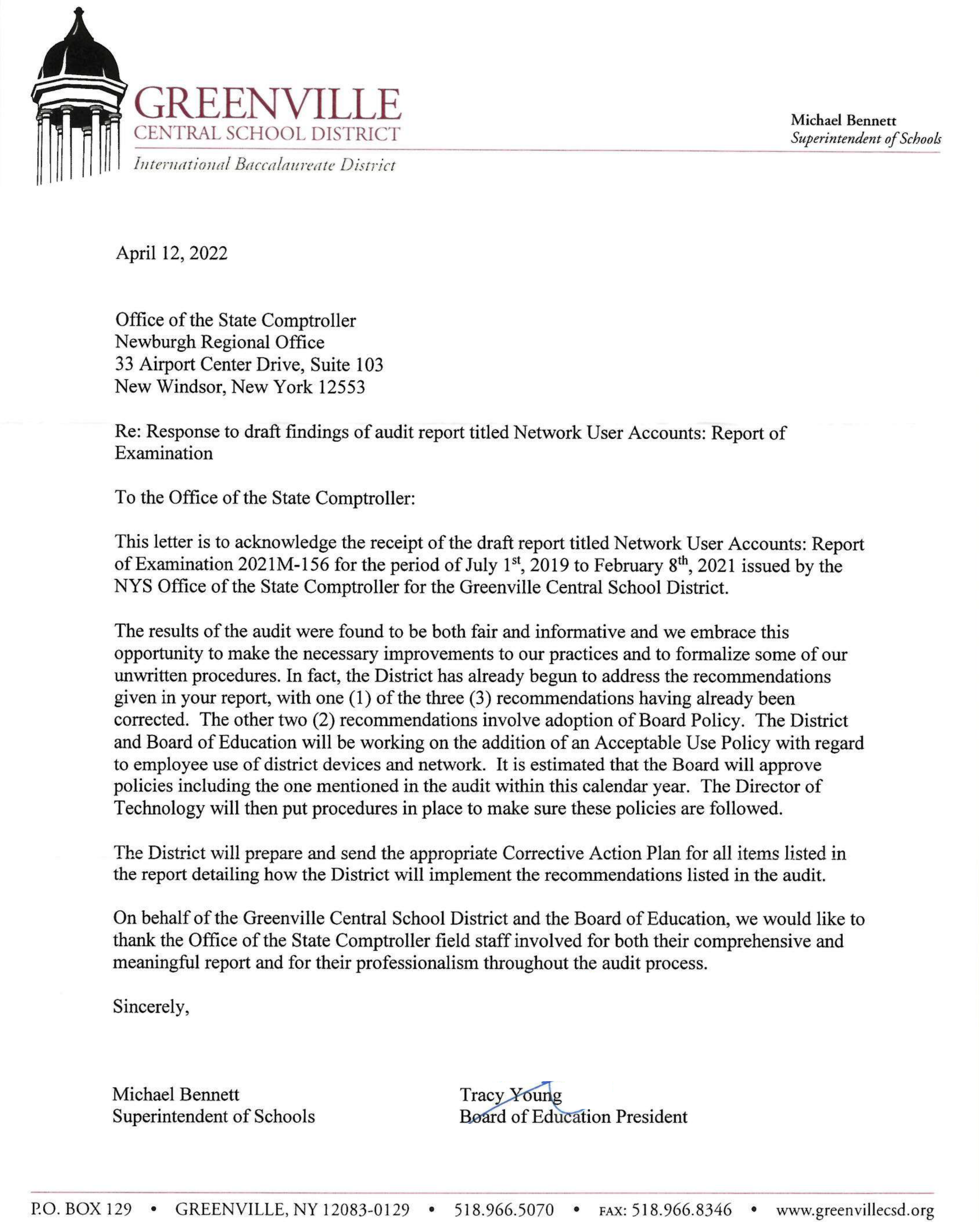
Appendix A: Personal Internet Use

Figure 1: Personal Internet Use

Type	Website
Real Estate	century21.com, realtor.com, zillow.com, custombuildingsystems.net, redfin.com, ashleyhomesllc.com
Employment	jobs.gsk.com, olasjobs.org
Entertainment	netflix.com, siriusxm.com
Shopping	fishgeeks.com, petsmart.com, instantlymodern.com, kellyspharmacyinc.com, venus.com, reallygoodstuff.com, kohls.com, lanebryant.com, allurebridals.com, maggiesottero.com, xenasbridal.com, oldermillennials.com
Personal Email	gmail.com, aol.com
News Media	abcnews.com, cbsnews.com, foxnews.com, today.com, nbcnews.com, timesunion.com, medicalnewstoday.com
Personal Online Banking	ulstersavings.com, comenity.net, ibx.key.com
Taxes	irs.gov,[a] turbotax.intuit.com
Travel	southwest.com

a) Although this website may be used for legitimate District purposes, the use we identified was personal in nature.

Appendix B: Response From District Officials



GREENVILLE
CENTRAL SCHOOL DISTRICT
International Baccalaureate District

Michael Bennett
Superintendent of Schools

April 12, 2022

Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Re: Response to draft findings of audit report titled Network User Accounts: Report of Examination

To the Office of the State Comptroller:

This letter is to acknowledge the receipt of the draft report titled Network User Accounts: Report of Examination 2021M-156 for the period of July 1st, 2019 to February 8th, 2021 issued by the NYS Office of the State Comptroller for the Greenville Central School District.

The results of the audit were found to be both fair and informative and we embrace this opportunity to make the necessary improvements to our practices and to formalize some of our unwritten procedures. In fact, the District has already begun to address the recommendations given in your report, with one (1) of the three (3) recommendations having already been corrected. The other two (2) recommendations involve adoption of Board Policy. The District and Board of Education will be working on the addition of an Acceptable Use Policy with regard to employee use of district devices and network. It is estimated that the Board will approve policies including the one mentioned in the audit within this calendar year. The Director of Technology will then put procedures in place to make sure these policies are followed.

The District will prepare and send the appropriate Corrective Action Plan for all items listed in the report detailing how the District will implement the recommendations listed in the audit.

On behalf of the Greenville Central School District and the Board of Education, we would like to thank the Office of the State Comptroller field staff involved for both their comprehensive and meaningful report and for their professionalism throughout the audit process.

Sincerely,

Michael Bennett
Superintendent of Schools

Tracy Young
Board of Education President

P.O. BOX 129 • GREENVILLE, NY 12083-0129 • 518.966.5070 • FAX: 518.966.8346 • www.greenvillecsd.org

Appendix C: 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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of the District's network user accounts and software updates and determine the adequacy of the policies and procedures.
- We ran a computerized audit script to examine the District's domain controller. We then analyzed the report by comparing user accounts to a list of current employees to determine whether any network account users were no longer employed by the District.
- We examined the web browsing histories on five of the 64 computers used by employees to determine whether employee Internet use complied with the District's AUP. We used our professional judgment to select five employees' computers based on their job duties that involved accessing PPSI.
- We also ran a computerized audit script on each of the five selected computers that retrieved installed software and operating system update dates. We reviewed the software versions to determine whether they were supported by vendors. We reviewed operating system update dates to determine whether the systems were up-to-date.

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

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

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 D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/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.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/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

www.osc.state.ny.us/local-government

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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller