New York State Comptroller
THOMAS P. DiNAPOLI

Rockville Centre Union Free School District

Information Technology

2023M-140 | March 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Rockville Centre Union Free School District

Audit Objective

Determine whether Rockville Centre Union Free School District (District) officials monitored users' compliance with the District's acceptable Internet use policy (AUP).

Key Findings

District officials did not monitor users' compliance with the District's AUP. Of the 37 network users we reviewed:

- Fifteen network users (41 percent) accessed websites, such as shopping, entertainment and social media, on District computers although the District's regulations for acceptable Internet use and computer resources and data management state that personal use is prohibited. As a result, the likelihood that a user's Internet browsing exposes the District to malicious software that may compromise data confidentiality, integrity or availability is increased.
- Fifteen network users (41 percent) did not have signed forms acknowledging they received and reviewed the District's AUP. This diminishes accountability and the District's ability to protect District computers and the data contained therein.
- Six nonstudent network users (22 percent) did not receive information technology (IT) security awareness training. As a result, the risk that users will not understand their responsibilities and put personal, private and sensitive information (PPSI) on District computers at greater risk of misuse or loss is increased.

Key Recommendations

- Monitor network users' Internet use on District computers and enforce compliance with the acceptable Internet use and computer resources and data management regulations.
- Limit the use of IT resources to only include District activities.

Audit Period

July 1, 2021 – December 22, 2022. We extended our audit period back to June 19, 2019 to review Internet history data.

Background

The District serves the Town of Hempstead in Nassau County. The District is governed by a five-member Board of Education (Board) that is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District's IT environment is managed by the IT Director who is the designee responsible for monitoring and examining all network activities to ensure the proper use of all IT systems. The IT Director reports to the Central Administration, which includes the Superintendent and the Assistant Superintendents for Finance and Operations; Special Education and Pupil Personnel Services; Curriculum and Instruction; and Human Resources.

Quick Facts	
Deployed Computers	1,000
Computers Reviewed	10
Network Users on Reviewed Computers	37
Total Webpage Addresses Reviewed	144,798
Total Personal Use Webpage Addresses Identified	10,044

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

Monitoring Acceptable Internet Use

To help protect school district (district) computers, district officials should limit and monitor for personal Internet use on those computers because it may increase the risk of exposure to malware, which could compromise PPSI[1] that resides on a malware-infected computer. PPSI could also be compromised if someone uses an infected computer to access it.

An AUP and other IT policies define a district board's expectations for appropriate user behavior to help protect district computers and the data contained therein. A district's AUP should describe appropriate and inappropriate use of district computers, including the Internet use on them, management's expectations concerning personal use of district computers and user privacy, and consequences for violating the AUP.

How Should District Officials Monitor User Compliance With the Acceptable Use Policy on District Computers?

District officials should monitor and analyze users' Internet use on district computers for signs of possible violations or imminent threats of violations of their AUP, other IT security policies, or standard security practices. Monitoring user compliance with AUPs involves regularly collecting, reviewing and analyzing district computer activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Officials should develop procedures for routinely monitoring Internet usage. Web filtering software can be used to help block, record and monitor access for unacceptable websites and limit access to sites that do not comply with a district's AUP. IT officials should communicate the AUP to all users and other individuals (e.g., consultants, vendors) who utilize the district's computers and Internet to perform their job duties and responsibilities.

District officials should provide IT security awareness training that explains the proper rules of behavior for using the district's computers and the data contained therein and communicate the policies and procedures that need to be followed.

The District's AUP consists of policies and regulations for acceptable use and for computer resources and data management that state that computerized information resources, and access to these resources, are for staff to enhance educational programs, further District goals, conduct research and communicate with others. The District's AUP, revised in 2022, stipulates that the use of the computer system is conditioned upon written agreement to the policy and any regulations adopted to ensure acceptable use of the computer system. The computer resources and data management policy and regulation state that the

1 PPSI is any information to which unauthorized access, disclosure, modification, or use – or disruption of access or use – could have or cause a severe impact on critical functions, students, employees, customers or third-party entities.

Superintendent (or his designee) should provide training to employees for proper use of the network, development of staff in computer skills and appropriate use of computers. The regulations for both the AUP and the computer resources and data management policies indicate that use of District computer resources and the Internet for anything other than school or work-related activities is prohibited. The regulation for computer resources and data management also indicates that the Superintendent or his designee should monitor and examine all network activities to ensure the proper use of all IT systems.

Officials Did Not Monitor District Computer Activity to Help Ensure Acceptable Internet Use

Officials did not monitor District computer activity for personal use and did not monitor user activity on those computers to help ensure acceptable Internet use. In the Internet history data on 10 District computers, we identified 37 network user accounts that were used to access the Internet. Based on our review, we determined that 15 of the 37 network user accounts (41 percent) were used to access the Internet for personal use, all of which was prohibited by the District's AUP and computer use and data management regulations. This prohibited Internet use included accessing websites related to online shopping, entertainment, travel, personal banking, college searches, real estate searches and job searches (Figure 1).

We reviewed 12,594 webpage address records, including the 10,044 we identified as personal use in Figure 1 and 2,550 that we determined were for District use. We discussed the webpage addresses with the IT Director and the Assistant Superintendent for Finance and Operations (Assistant Superintendent).

The Assistant Superintendent said that the AUP regulation has not been revised since 2010 and needs a thorough review and update to correspond with the language in the AUP, which was updated

Figure 1: Personal Website and Web Search Categories

Website Category	Number of Times Website Category Appeared
Online Shopping[a]	5,148
Entertainment	1,953
Informational search	842
Travel	733
Healthcare and Insurance	422
College search	287
Bill Payment	255
Personal Banking	238
Personal Email	128
Job search	30
Social Media	4
Online Gambling	2
Real Estate search	2
Total	**10,044**

a Includes shopping for a car and boat, as well as personal and household items.

in 2022. The IT Director and Assistant Superintendent said the District's only unacceptable personal use, based on the AUP and not the corresponding regulations, is the transmission of confidential student or staff information, and that as long as student or staff confidential information was not transmitted, the personal use is considered acceptable. The Assistant Superintendent further explained that while some webpage addresses were for personal use, the AUP did not establish any restrictions on personal use or clearly define what kind of personal use was prohibited. The Assistant Superintendent said that although the associated AUP regulation expands on prohibited activities for computerized information resources, he thinks it is unclear whether Internet activity is included in that classification. However, we disagree with the Assistant Superintendent because the AUP specifically cites "the Internet" as being included in the "various computerized information resources" the Board will provide to staff. The Assistant Superintendent agreed that the AUP regulation indicates that Internet use for purposes other than school-related business is prohibited, so some of the webpage addresses we found were prohibited. However, he said that without asking each user about each webpage address, it would be impossible for District officials to verify acceptable and unacceptable use.

While the District's AUP lacks clarity regarding acceptable use of the Internet, the associated AUP regulation states that personal use of the Internet is prohibited and the computer resources and data management regulation indicates that use of the Internet is for school and work-related activities only, so none of the personal use identified was acceptable. Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity or availability. For example, the Internet history data associated with a former District nurse comprised 39 percent of the personal Internet use we identified. If this personal use exposed the computer to malicious software, confidential data could have been compromised, including student and employee medical information or other PPSI available to District nurses.

Although the computer resources and data management regulation required that network activities, including Internet use on District computers, be monitored and examined, the District had no procedures for monitoring Internet use. The IT Director did not monitor Internet use on District computers because he said that the monitoring intended by the AUP and computer resources and data management regulations was accomplished through the District's use of software and services that provided web filtering and continuous monitoring of computer behavior and network traffic that generated alerts for suspicious, malicious or inappropriate activities. He also explained that sites used for legitimate business purposes would not generate alerts because the software and services cannot differentiate between business and personal use. While the web filtering and third-party monitoring can help mitigate instances of inappropriate browsing or Internet

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity or availability.

use, periodic reviews of web history would provide a more definitive examination of activity to identify inappropriate use.

District officials did not adequately monitor Internet use on District computers for non-District activities, which resulted in personal Internet use occurring and remaining undetected. All 10 computers were routinely used to access data that contained confidential information, including:

- Financial systems,
- Payroll records,
- Online bank accounts,
- PPSI related to employees and students, including social security numbers, full names, dates of birth and home addresses.

Network users logging in on these computers could unknowingly visit infected websites and, as a result, the District's computers and PPSI were at a higher risk of exposure to breach, damage, loss or misuse. Furthermore, the lack of monitoring allowed higher risk Internet use to occur undetected, such as social media, shopping and online gambling sites, which increased the possibility of a computer being exposed to malware. Lastly, personal Internet use could have reduced employee productivity while they used District resources.

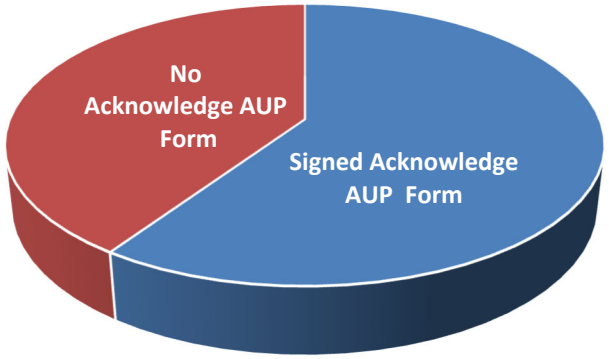
Network Users Did Not Acknowledge the Acceptable Use Policy

According to the AUP, the District realizes its obligation to teach and ensure responsible and safe use of the District's network, and stipulates that the use of the computer system is conditioned upon written agreement to the policy and any regulations adopted to ensure acceptable use of the computer system.

Network users did not sign the acknowledgement form as required by the District's AUP. To ensure that each network user had a written agreement, we requested the signed acknowledgement forms for the network users of the 37 network user accounts identified in our Internet history results. The IT Director provided us with signed forms for 22 (59 percent) of the 37 network user accounts (Figure 2). The remaining 15 network user accounts (41 percent) did not have signed acknowledgement forms, including:

FIGURE 2

Acknowledged AUP Form



- Six accounts assigned to current and former employees,
- Five shared accounts, and
- Four accounts assigned to former students.[2]

The IT Director said he could not provide the acknowledgement forms for three former employees because the District shreds the forms when employment is terminated, and the three current employee network users did not have signed forms because they were not assigned District IT equipment. Although the computer resources and data management policy applies to all users of the District's computer network, the District's procedure is to only have an acknowledgement form signed when a computer is assigned to a user instead of when a network user account is assigned. Creating a network user account for an individual that is not required to acknowledge the acceptable use guidelines increases risk to the network. For example, we determined that one current employee logged into a laptop assigned to a nurse and accessed the Internet for personal use. The five shared user accounts were not assigned to a specific network user, such as a general account used for student exams and a general high school teacher account. District officials did not track who accessed shared accounts because they were used by multiple people for various purposes. Given that the use of shared accounts reduces accountability because usernames and passwords are shared among two or more users, often guests or other temporary or intermittent users, use of these accounts should be closely monitored and

2 Although our selected audit sample comprised only equipment assigned to employees whose job duties included accessing PPSI or other confidential information, some laptops in our sample were previously assigned to former students and had Internet history data files pertaining to their network use.

users should be required to acknowledge the AUP prior to being provided the shared accounts access information. The IT Director said the forms for network user accounts assigned to former students were not available because the District shreds them when students leave the District.

Assigning users a network user account and allowing them to access the network without first requiring them to acknowledge the AUP and its directives diminished accountability and the District's ability to protect District computers and the data contained therein, putting the District's network at risk.

Some Users Did Not Receive IT Security Awareness Training

We requested the IT security awareness training records for the 27 individual nonstudent network users of the 37 network user accounts identified with Internet history results. The IT Director provided us with training records for 21 network users, including 10 users identified with personal Internet use. Although the computer resources and data management policy and regulation require the Superintendent's designee to ensure training is provided to employees for proper use of the network, the IT Director could not provide training records for the other six users. Furthermore, five of the six users that did not receive training also did not have a signed AUP acknowledgment form.

The IT Director said that one user was a new employee whose employment started in November 2022, and another user was out on extended leave and recently returned in 2023, so neither received the training because training is provided in September at the start of the school year. He also said that a third user did not have a training record because the person is no longer employed by the District, and the previous training software program did not record employee training attendance or completion. The Internet activity we identified and reviewed for these three nonstudent network users corresponded with the explanations provided by the IT Director. However, the remaining three nonstudent network users should have been provided IT security awareness training but were not. The IT Director said these three users were not permanent employees and were not required to take the training. However, the AUP does not indicate that temporary employees with access to the District's network are not required to receive IT security awareness training. Allowing nonstudent network users to access the District's network without training increases the risk that users will not understand their responsibilities, or how their Internet browsing could put computers and the data residing on them – including PPSI – at greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

The IT Director should:

1. Monitor network users' Internet use on District computers and enforce compliance with the District's regulations.
2. Limit the use of IT resources to include only District activities.
3. Ensure that all network users sign an AUP acknowledgement form as required by District policy, including those using a shared network account. Signed AUP acknowledgment forms should be retained in accordance with the District's record retention policy.
4. Ensure all nonstudent network users are provided with IT security awareness training.

Appendix A: Response From District Officials

ROCKVILLE CENTRE UNION FREE SCHOOL DISTRICT

Kelly Barry, President • Donna Downing, Ph. D., Vice President • Janet Gruner, Secretary • Tara Hackett, Trustee • Erica Messier, Trustee

Matthew Gaven, Superintendent of Schools

February 26, 2024

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

Dear Office of the New York State Comptroller:

The Board of Education and Administration of the Rockville Centre Union Free School District would like to take this opportunity to thank the field staff of the Comptroller's Office for their courtesy in conducting their audit and in working with District staff. Feedback and recommendations for improvement are always welcomed by the District as we strive for continuous improvement in our operations and safeguarding access through our information technology resources.

Please consider this letter the District's response to the Report of Examination of Information Technology within the Rockville Centre Union Free School District for the period of June 19, 2019 through December 22, 2022.

The District has continued to upgrade and monitor internet activity each year by adding software and hardware designed to limit access to websites, monitor web search activity and to detect malware and phishing targeting of District technology resources. In addition, there have been a number of training activities implemented for District users including addressing phishing, malicious software and protection of personally identifiable information (PII). The District acknowledges the need to monitor user internet activity to safeguard District resources and information and appreciate the recommendations provided within this audit report. In response to the recommendations, the District will review both the acceptable use policy and its associated regulation to clarify any inconsistencies, ensure all network uses are provided with IT security awareness training and ensure all network users acknowledge the acceptable use policy.

Again, thank you for your work and recommendations for improvement in safeguarding District Information Technology resources. The Board and District Administration are committed to the continuation of providing appropriate training of the District's computer network users and compliance with the District's acceptable use policy to reduce exposure to malicious software that may compromise technology resources.

Respectfully,

Matthew Gaven
Superintendent of Schools

Board of Education • 128 Shepherd Street • Rockville Centre, NY 11570 • 516-255-8920 • www.rvcschools.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 identified and evaluated the District's AUP and related regulations to gain an understanding of internal controls over Internet use on the District's network.
- We interviewed the IT Director to gain an understanding of internal controls over Internet use on the District's network.
- We analyzed Internet history data on 10 District computers, including six desktops and four laptops, assigned to the Board President and eight employees, including secretaries and nurses, whose job duties required them to access PPSI or other confidential information. District computers were shared among users, allowing them to use more than one computer with their network user account log-in credentials. We used our professional judgment to select the Board President and eight employees because each has access to sensitive or confidential information.
- On December 20, 21 and 22, 2022, we used a computerized web history exporter script to retrieve Internet history files from the six desktop computers and four laptop computers assigned to the nine individuals from our sample.
- We converted and analyzed the exported web history data for accessed websites and followed up on any questionable results with the direct employee or department head. We discussed the results with the IT Director and Assistant Superintendent to determine whether the Internet use complied with District policy.
- We reviewed 12,594 webpage addresses with officials and employees to help distinguish personal Internet use from District use. We discussed the webpage addresses identified as being for personal Internet use with the IT Director and Assistant Superintendent to obtain explanations.

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties