New York State Comptroller
THOMAS P. DiNAPOLI

Oceanside Union Free School District

Monitoring Internet Use

2022M-195 | March 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Oceanside Union Free School District

Audit Objective

Determine whether Oceanside Union Free School District (District) officials monitored employees' compliance with the acceptable Internet use policy (AUP) on the District's network.

Key Findings

District officials did not monitor employee compliance with the acceptable Internet use policy on the District's network. In addition to finding sensitive information technology (IT) control weaknesses, which we communicated confidentially to officials, we found that:

- Six of 40 employees used District computers to access websites, such as shopping, entertainment, personal email, online gaming and social networking, in violation of the District's AUP. Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity or availability.

Key Recommendations

- Monitor employee Internet use on District computers and enforce compliance with the AUP.

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

Background

The District serves the Town of Hempstead in Nassau County. The District is governed by a seven-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 District's day-to-day management under the Board's direction.

The District's Internet use is managed and monitored by the Instructional IT Director (IT Director), who reports to the Assistant Superintendent for Curriculum, and the IT Director of Data Assessment and Administrative Services (IT Director 2), who reports to the Superintendent. The District's IT specialist works with the IT directors and reports to the Assistant Superintendent for Business (Assistant Superintendent).

Quick Facts	
District Computers in Active Use	967
Computers Reviewed	27
District Employees	1,159
Employees Who Used the Internet on Reviewed Computers	40

Audit Period

July 1, 2021 – August 4, 2022

Monitoring Internet Use

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

IT policies define a district board's (board's) expectations for appropriate user behavior to help protect data and IT systems. A district's AUP should describe appropriate and inappropriate use of IT resources, including Internet use, management's expectations concerning personal use of IT equipment and user privacy, and consequences for violating the AUP.

How Should Officials Guide and Monitor Employee Compliance with the Acceptable Internet Use Policy?

District officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of IT security policies, AUPs, or standard security practices. Monitoring compliance with AUPs involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

The District established an AUP that defined the Board's expectations for appropriate user behavior and the Board's right to ensure compliance with the AUP through electronic monitoring of network and Internet use. The AUP states that computer network and Internet users may not access private accounts or subscribe to mailing lists, bulletin boards, chat groups or commercial services without the authorization of a staff member designated by the IT Director.

Other inappropriate, unauthorized uses included, but were not limited to, purchasing personal items using the District's network and using District-owned hardware for commercial activities, product advertising, political lobbying or any other activities that were not directly related to an approved educational or job-related use. Personal usage such as shopping, banking, visiting Internet radio sites, printing personal materials, playing computer games, watching videos and streaming media was prohibited while on the District's network, because these activities could significantly degrade bandwidth.

According to the AUP, the District generally defined social media to include websites, web logs, wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the District community that did not fall within the District's electronic technology network. Using

[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.

these media during the time that employees should have been performing District responsibilities, or while they were using District-owned equipment, was discouraged. Employees who violated the District's AUP were subject to discipline, as stated in the policy.

Officials Did Not Monitor Employee Compliance with the AUP

Each time an employee logged into the District's computer network, they acknowledged that they read, understood and would abide by the AUP. However, District officials did not monitor employees' Internet use or compliance with the AUP.

We analyzed Internet history data on 27 District desktop computers assigned to employees whose job duties required them to access PPSI or other confidential information. District computers were shared among employees, allowing them to use more than one computer with their network user account log-in credentials. From the Internet history data results, we identified 40 employee network user accounts used to access the Internet from the 27 computers. Although all 40 employees clicked on the policy acknowledgement banner daily, and all were aware of the AUP, we found that six employees used District computers for personal Internet use.

During our audit period of July 1, 2021 through August 4, 2022, employees' personal Internet use included accessing websites related to social media, travel, online shopping,[2] entertainment, personal email, informational websites, real estate searches, online gaming, personal banking, personal subscriptions and healthcare services. In addition, we found Internet browser searches related to personal use (Figure 1).

Figure 1: Personal Website and Web Search Categories

Website Category	Number of Times Website Category Appeared
Social Media	670
Travel	154
Online Shopping	80
Entertainment	68
Informational Website	15
Real Estate	15
Gaming	14
Personal Email	11
Personal Health	5
Personal Banking	3
Personal Subscription	3
Total	**1,038**

Of the seven network user accounts, two[3] were used by a Department of Community Activities (DOCA)[4] employee on three District computers. Not only did we find personal Internet use on these three District computers, but also this employee's Internet use accounted for 98 percent of the personal Internet use that we identified.

[2] Includes car shopping as well as shopping for personal and household items

[3] The IT Specialist explained that the District created an initial network user account for this part-time employee and later disabled it and created another network user account when the employee became a full time district employee.

[4] DOCA – Department of Community Activities - offers youth activities, continuing education and Children's After-School Recreational, Educational and Social Program for children's after-school needs, summer programs, community sports, and special events to the District's community.

In addition, of the seven District computers with personal Internet use, we found that the Internet browsing history of five computers (which included the three computers previously mentioned) had websites related to antimalware software.[5] We could not definitively determine whether this website activity appeared in the Internet browsing history due to possible suspicion of malware infection. However, the IT specialist told us that IT department staff (IT staff) installed this particular antimalware software only on computers suspected to have malware infections or because employees complained of computers working slowly.

Because IT staff installed this software only on computers that they suspected had malware infections, they should have notified these employees to discontinue their personal Internet use. This personal use could have caused the computers to malfunction, and it put the computers and the entire network at greater risk of malware infection. However, because IT staff did not monitor employee Internet activity, they did not detect or correct inappropriate personal use.

The IT Director told us that the District heavily monitored student compliance with the AUP and used web-filtering and firewalls to prohibit access to some websites. IT staff used website access logs that documented all student Internet activity and alerted IT staff to any access attempts to restricted websites. Students are always monitored, whether they are on the District's network or not. However, the District's AUP was not only applicable to students; it was applicable to all users. The IT Director said that there were some prohibited websites and firewalls for employees, but not on the same level as students, and some websites had to be open for things such as purchasing.

However, IT staff told us that employees had an "open network," meaning that the District did not monitor employee personal Internet use or prohibit access to any websites not related to District business. The IT Director agreed that the personal Internet use that we found was not an acceptable use of District resources. But the IT Director also told us that while Internet access settings for staff were updated to reflect the District's expanded use of things such as social media, the AUP was not modified to meet the current Internet-use environment needed for District staff.

All seven computers with personal Internet use were routinely used to access the District's financial systems; payroll records; employees' social security numbers, full names, dates of birth and complete home addresses; the Districts' online bank accounts; and some PPSI related to students who were enrolled in DOCA programs. Furthermore, lack of monitoring allowed higher-risk Internet

[5] Antimalware (or antivirus) software is a program designed to detect and remove viruses and other kinds of malicious software from a computer or laptop.

use to occur undetected, which increased the computers’ exposure to malware.[6] Ultimately, five of the 27 computers required additional software to resolve suspected infections.

We discussed our audit results with the Assistant Superintendent, IT Director, IT specialist and DOCA supervisor. The IT specialist told us that the restrictions for employees were very limited, and the District did not have any filters or other tools to monitor Internet activity on District computers for nonwork-related searches or other personal use.

The IT Director told us that, though the District used web-filtering software to block access to some prohibited websites, websites that also could be used for personal purposes (such as shopping, real estate and travel) were not blocked because they were used occasionally for business or educational purposes.

Although employees could access websites for personal purposes, the IT Directors did not ensure that IT staff periodically reviewed Internet use logs for appropriateness. Therefore, strict filtering or website block-listing might not be beneficial. The IT Director told us that IT staff would evaluate whether they could add a security layer to Internet access permissions for noninstructional staff to ensure they complied with the AUP. However, relying on an additional filter security layer would not be as beneficial as implementing a monitoring process, such as periodic review of Internet use logs.

Internet browsing increases the likelihood of computers being exposed to malware, which may compromise PPSI. An employee could unknowingly visit an infected website and, as a result, the District’s IT assets and any PPSI they hold would have a higher risk of exposure to breach, damage, loss or misuse.

The IT Director also told us that the District previously prohibited personal email use, but no longer did so. She said that personal emails possibly were not blocked because the District’s email was heavily filtered, which sometimes blocked even legitimate emails. Therefore, employees used their personal emails for official District business. However, using personal email violated the AUP and circumvented the District’s email filtering, which diminished the District’s ability to enforce compliance with the AUP.

While the IT Director told us that the District prohibited students from accessing some websites, it did not ensure that employees complied with the AUP. If the AUP had indicated how IT staff should restrict and monitor personal use, and the consequences for noncompliance, they would have had clear instructions on how to properly monitor Internet use and apply consequences for AUP violations.

[6] Malware is software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system. Common examples of malware include viruses, worms, Trojan horses and spyware.

Also, providing employees with an open network without monitoring for non-District activities allowed the Internet use that we identified to occur and remain undetected. This personal Internet use could have reduced employee productivity while they used District resources. Furthermore, when actual practices are not in line with the AUP, and known violations are openly tolerated, the District's ability to enforce compliance could be diminished.

What Do We Recommend?

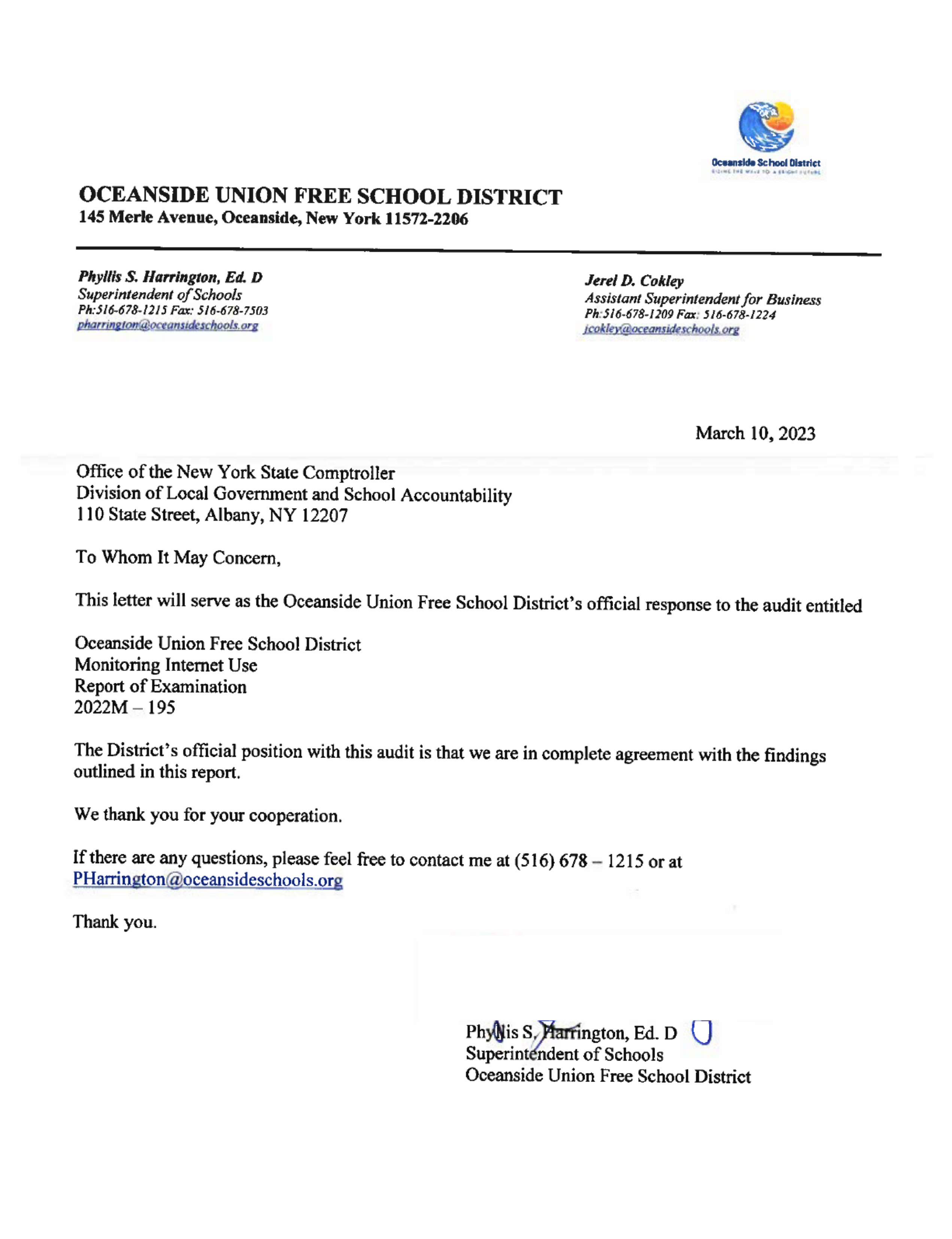
The Board should:

1. Ensure proper IT internal controls are in place and emphasize the importance of complying with the AUP.

The IT Directors should:

2. Monitor employee Internet use on District computers and enforce compliance with the AUP.
3. Limit the use of District IT resources to include only District activities.

Appendix A: Response From District Officials



Oceanside School District
RIDING THE WAVE TO A BRIGHT FUTURE

OCEANSIDE UNION FREE SCHOOL DISTRICT
145 Merle Avenue, Oceanside, New York 11572-2206

Phyllis S. Harrington, Ed. D
Superintendent of Schools
Ph:516-678-1215 Fax: 516-678-7503
pharrington@oceansideschools.org

Jerel D. Cokley
Assistant Superintendent for Business
Ph:516-678-1209 Fax: 516-678-1224
jcokley@oceansideschools.org

March 10, 2023

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, Albany, NY 12207

To Whom It May Concern,

This letter will serve as the Oceanside Union Free School District's official response to the audit entitled

Oceanside Union Free School District
Monitoring Internet Use
Report of Examination
2022M – 195

The District's official position with this audit is that we are in complete agreement with the findings outlined in this report.

We thank you for your cooperation.

If there are any questions, please feel free to contact me at (516) 678 – 1215 or at PHarrington@oceansideschools.org

Thank you.

Phyllis S. Harrington, Ed. D
Superintendent of Schools
Oceanside Union Free School District

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

- We identified and evaluated the District's AUP to gain an understanding of internal controls over Internet use on the District's network.
- We interviewed the Assistant Superintendent, IT Directors and IT specialist to gain an understanding of internal controls over Internet use on the District's network.
- We reviewed a list of District computers in active use as of July 2022, provided by the IT specialist, and used our professional judgment to review the Internet browsing history on 20 desktop computers. We chose these computers because they were used by employees whose job duties required them to access PPSI or other confidential information. We later added seven more computers (used by DOCA employees) to our sample, thereby increasing our total sample to 27 desktop computers, to analyze the Internet browsing history data. Our expanded sample encompassed all computers used by DOCA employees.
- On July 14, July 15 and August 4, 2022, we used a computerized web history exporter script to retrieve Internet history files from our sample of 27 computers.
- We converted and analyzed the exported web history data for accessed websites and discussed the results with the Assistant Superintendent, IT Director, IT specialist and DOCA supervisor to determine whether employee Internet use violated the District's AUP.

Our audit also examined the adequacy of certain sensitive 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 the 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 C: 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

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