



Manhasset Union Free School District

IT Asset Management

S9-22-15 | March 2023

Contents

- Report Highlights 1**

- IT Asset Management 2**
 - How Should District Officials Inventory and Safeguard IT Assets? . . . 2
 - Officials Did Not Appropriately Inventory or Safeguard IT Assets . . . 3
 - What Do We Recommend? 7

- Appendix A – Response From District Officials 8**

- Appendix B – Audit Methodology and Standards 10**

- Appendix C – Resources and Services 12**

Report Highlights

Manhasset Union Free School District

Audit Objective

Determine whether Manhasset Union Free School District (District) officials appropriately tracked, inventoried and safeguarded information technology (IT) assets acquired or in use during the audit period

Key Findings

District officials did not appropriately track or inventory IT assets, maintain complete IT inventory records or establish adequate controls to safeguard IT assets. As a result, officials cannot assure taxpayers that money invested in IT assets has been appropriately spent or safeguarded.

We selected 50 IT assets to confirm their location and that they were inventoried, and 10 additional IT assets to confirm they were inventoried. We found 20 percent of the sampled assets were not properly accounted for. Specifically:

- Six assets (one laptop and five Chromebooks) with a combined value of approximately \$2,165 could not be located.
- Six assets (five interactive displays and one Chromebook) with combined purchase prices of approximately \$27,800 were not inventoried.

In addition, annual inventories were not adequately conducted, IT equipment was susceptible to environmental damage, and officials did not adopt a comprehensive written policy for establishing and maintaining IT equipment inventory.

Key Recommendations

- Ensure District inventory records are complete and include the detail necessary to adequately track and locate IT assets.
- Perform annual and complete physical inventories and compare results to inventory records.

District officials generally 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 elected five-member Board of Education (Board) is responsible for the general management of the District.

The Superintendent serves at the Board's direction and is responsible for day-to-day management.

The IT Director is responsible for overseeing the IT Department, including IT asset inventory management.

The IT Director oversees an IT Manager as well as seasonal (summer) student workers assigned to the IT Department.

Quick Facts

District	
Enrollment	3,051
Staff	879
Approximate Cost of IT Assets Purchased or Leased in Our Audit Period	\$2.53 million

Audit Period

July 1, 2019 – March 31, 2022. We expanded our audit period through July 11, 2022 to observe inventory at the District.

IT Asset Management

School districts purchase a wide variety of IT equipment, such as interactive displays and desktop computers, as well as highly portable items, such as monitors, laptops and tablets. These assets can make up a significant portion of a district's IT asset inventory, in both value and number. School district officials are responsible for providing oversight to ensure that assets are protected from loss, inventory records are current, and assets can be easily located.

With the onset of the COVID-19 pandemic, school districts acquired a significant number of IT assets to transition to remote and hybrid learning. This influx of new and often highly portable IT assets highlighted the importance of tracking and inventorying practices to ensure that taxpayer funds are appropriately spent and safeguarded.

How Should District Officials Inventory and Safeguard IT Assets?

A school board should adopt a comprehensive written policy that sets forth guidelines and procedures for establishing and maintaining IT asset inventory. Although some IT assets could be considered fixed assets, IT assets' portability and access to a district's network and/or confidential data poses a distinct risk of loss or misuse. Given this risk, school district officials should establish a separate, well-defined policy that includes guidance for school district officials to maintain detailed, up-to-date inventory records for all IT assets including:

- Adding new equipment to the inventory,
- Notifying the IT Department when equipment is reassigned, lost or stolen,
- Documenting and updating the inventory for equipment disposal, and
- Annually reviewing the physical inventory.

Inventory records should include a description of each item including the make, model and serial number; the name of the individual to whom the device is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the initial cost, depreciation and acquisition date.

In addition, school district officials should verify the accuracy of IT asset inventory records through annual physical inventory counts. Devices should be periodically examined to assess their condition and to verify accurate location information in the inventory records. Maintaining complete and up-to-date IT asset inventory records also helps a school board develop and implement an effective IT equipment replacement plan. To safeguard IT assets from loss, theft or misuse, IT assets should be in a locked and secured area with environmental controls such as smoke detectors, fire alarms and extinguishers, and protection from water damage.

Officials Did Not Appropriately Inventory or Safeguard IT Assets

Although the Board-adopted Capital Asset Accounting Policy (Accounting Policy) and Authorized Use of School-Owned Materials and Equipment Policy¹ (Equipment Policy) provide direction for officials to track and inventory assets, the Board did not adopt a comprehensive written policy specifically for IT equipment inventory.

According to the Accounting Policy, capital assets are non-consumable assets with a normal service life of more than two years, and an inventory record for equipment costing in excess of \$500 shall be inventoried and equipment costing less than \$500 shall be inventoried for accountability purposes if requested by the responsible program administrator. In addition, the Equipment Policy requires the IT Department to maintain records for all equipment loaned for use. These records shall include the date the equipment was loaned, to whom it was loaned, and the date of expected return and actual return. Neither policy provides directions to ensure all IT assets are tracked and inventoried appropriately.

The Accounting Policy states the following information must be maintained on the equipment/fixed asset inventory:

- Name and description,
- Location of equipment,
- Serial and other identification number,
- Cost of the asset at acquisition, and
- Acquisition date.

Furthermore, the Accounting Policy requires certain attributes to be recorded that do not necessarily aid in tracking and inventorying IT assets but are important for other operational needs. For example, date of acquisition and cost do not aid in tracking an asset but are useful for determining overall cost or age of assets, which in turn, could ensure appropriate insurance coverages are maintained and assist in planning for replacement of assets reaching the end of their useful life. Although the District's accounting records have the costs, acquisition date and vendor information for IT assets, this information is not easily compiled for inclusion in the District's IT asset inventory records and cannot easily aid in planning for future IT asset investments. Therefore, the cost and age of all IT assets currently in use by the District was undetermined at the conclusion of our fieldwork.

According to the IT Director, in September 2021, during the District's transition to a new inventory system, the IT Department lost information from the previous inventory application due to a network-wide third-party data issue. Further, they

¹ Policy 6610, adopted September 23, 2004, and Policy 8330, adopted March 20, 1997 and last updated on December 13, 2018.

had other network security concerns that took precedence over ensuring the IT asset information was updated. As a result, not all information from the old application was recorded in their new inventory system.

Inventory Records – The IT Director and the IT Manager maintain one inventory list for the District’s IT assets. In addition, the Business Office contracts with a third-party vendor to provide an insurance valuation of all District capitalized fixed assets, which should include some IT assets. This valuation is known as the Accounting Detail Report. We reviewed the IT Department’s inventory list and the Business Office’s Accounting Detail Report and found both lists contained all attributes required by the Accounting Policy.

However, the Business Office’s Report did not contain all the District’s IT assets and the IT Department’s inventory list did not always contain adequate information to sufficiently track and/or identify the District’s IT assets. For example, there were numerous missing, incomplete and/or inaccurate information for individual entries on the IT Department’s inventory list, such as an IT asset’s serial number, acquisition date, cost, or location. Specifically:

- Serial numbers were missing for 164 out of 6,287 items. The Director told us they had not entered all the information into the new system after the network-wide data issue in September 2021 because they had more pressing concerns. Further, he told us they no longer have access to information in the previous inventory application, and as a result some information may be missing.
- Duplicate serial numbers were found for 26 assets recorded. The IT Director told us duplicate assets were likely recorded in error.

Further, the IT Department does not reconcile their list to the Business Office’s Accounting Detail Report. The lack of a reconciliation process only adds to the deficiencies in the respective lists, and does not allow for a single, complete master listing of IT assets.

In our physical test of 50 IT assets, six assets (five interactive displays and one Chromebook), with a total purchase price of approximately \$27,800 were not recorded in either department’s inventory records. All 10 assets additionally identified during our walk-through and inspection of the District were appropriately recorded in the IT Department’s inventory list; however, one Chromebook costing \$315 was not recorded on the Business Office’s Accounting Detail Report.

Annual Inventories –The IT Director told us he was aware of the policies and said that the IT Department inventories all equipment for accountability. Further, the IT Director and IT Manager explained that they directed the student workers to perform a physical inventory in August 2021. Both the IT Director and the IT Manager told us that although they provided the student workers guidance, they did not provide supervision during the physical inventory. As a result, they were

unaware of what was recorded until the inventory was completed and discovered it was not adequately performed.

We reviewed the results of that inventory and found that the physical inventory was only conducted at three of the four District buildings and did not include student devices or all IT assets in each of the District buildings. As a result, this physical inventory may have excluded approximately 70 percent of District IT assets in use. Further, the results of the physical inventory did not always include asset tags, serial numbers, locations or assigned user. For example, 669 serial numbers (37 percent) and 1,763 assigned users (97 percent) were missing from the 1,816 individual assets recorded.

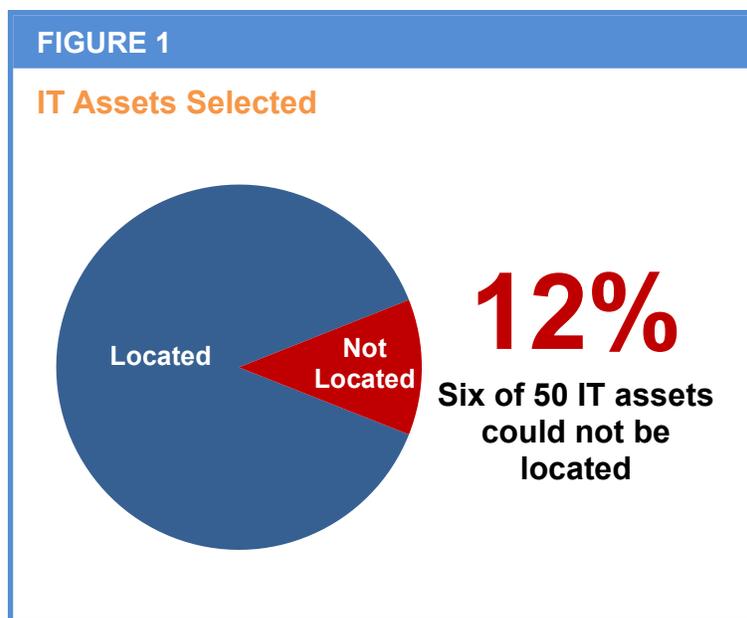
Safeguarding Assets – The IT Director could not locate six of the 50 assets we selected (12 percent) to physically confirm were in the District’s possession (Figure 1).

These assets included one laptop and five Chromebooks with a combined cost of approximately \$2,166.

The IT Director told us the laptop was assigned to a District teacher but could not provide documentation to support that it was in the teacher’s possession. He also told us the Chromebooks were student-assigned devices; however, the Chromebooks had not connected to the District network since at least December 2021. He further explained that when a student-assigned device is not returned, District staff will email and/or call the student’s family to return the device.

However, they did not have evidence of this assertion.

In addition, during our building walk-through and inspection of District IT assets, we observed water leakage and associated damage on the ceiling above



equipment in the main wiring closet at one of the elementary schools (Figure 2). The evidence of water leakage above IT assets, as well as the remnants of ceiling tile material on stored assets, indicates the IT hardware was susceptible to damage.

FIGURE 2

Water Leak and Ceiling Damage in Server Closet



a) Server room entry and stored IT assets.
b) Water leakage and damaged/crumbling ceiling above stored IT assets shown in photo a.
c) Closeup of deteriorated ceiling tile material on stored IT assets shown in photo a.

The IT Director did not maintain detailed up-to-date inventory records, provide adequate oversight of student workers directed to perform physical inventories or safeguard assets from loss or damage. As a result, District officials cannot be assured that IT assets are adequately accounted for and would be detected if lost, stolen, or misused. Further, complete, accurate, and up-to-date inventory records help District officials ensure that IT assets are properly insured, tracked through their life cycle and replaced as necessary. When inventory records are incomplete, and assets are not properly accounted for, District officials cannot ensure taxpayers that money invested in IT assets has been appropriately spent or safeguarded. Finally, IT system components should always be in a locked and secured area to further safeguard them from damage or loss.

What Do We Recommend?

The Board should:

1. Adopt a specific comprehensive written policy to appropriately track and inventory IT equipment. This policy should include guidance and processes for:
 - Maintaining detailed, up-to-date inventory records for all IT equipment,
 - Adding new equipment to the inventory,
 - Notifying the IT Department when equipment is reassigned, lost or stolen,
 - Documenting and updating the inventory for equipment disposal, and
 - Annually reviewing the physical inventory.
2. Require the IT Director to perform a physical inventory of all IT equipment, locate missing and unaccounted-for equipment and update inventory records accordingly.

The IT Director should:

3. Review and comply with applicable District policies.
4. Ensure District inventory records include the detail necessary to adequately track and locate an IT asset and that asset records minimally include the make, model and serial number; the name of the individual to whom the device is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the initial cost, depreciation and acquisition date.
5. Reconcile the IT Department list with the Business Office list and develop a single, master inventory list.
6. Update inventory records to track assets not currently in District records.
7. Perform a complete, annual physical inventory and compare the results to the inventory records. Take appropriate action to follow up on any discrepancies.
8. Ensure District personnel keep IT asset storage areas safe from environmental damage, such as water leakage.

Appendix A: Response From District Officials



MANHASSET PUBLIC SCHOOLS

Gaurav Passi, Ed.D.
Superintendent of Schools

January 5, 2023

VIA EMAIL TO [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
Division of Local Government and School Accountability
33 Airport Center Drive
New Windsor, NY 12553

Dear [REDACTED]

Thank you for your recent audit of the Manhasset School District's IT Asset Management processes and policies. Your audit sought to test whether we appropriately tracked and inventoried our information technology assets from July 1, 2019 – March 31, 2022. The District accepts and does not dispute the key findings in your report. We appreciate the recommendations you provided.

The overall context of the audited period is an important factor in understanding the issues facing the District during the audited time period. The report does not address the context of two unprecedented events the District faced during this timeframe. Specifically, we would like to note that the audited period covered the time of the COVID-19 pandemic's inception and when the District was a victim of a criminal ransomware attack.

- **COVID-19 Pandemic:** The COVID-19 pandemic commenced in March 2020 and created the instant requirement to provide continuity of learning to our students in a remote environment. To meet this imperative, the District faced an unprecedented need to rapidly increase IT assets and provide 1:1 technology tools for over 3,500 students, teachers, and teaching assistants districtwide. While the District's IT staff quickly and efficiently provided both the technology as well as the related training on the use of the equipment to ensure the continuity of instruction, we agree that the influx of essential equipment presented a record keeping challenge to the District. As noted in the report, the summer 2021 inventory did not include student Chromebooks (3,100) nor staff laptops (488) as these devices were in the hands of students and staff members for the summer. Together these devices account for approximately 57% of IT assets. We will share in our detailed corrective action report procedures introduced this year to

200 Memorial Place, Manhasset, New York, 11030
(516) 267-7705 – gpassi@manhassetsschools.org – www.manhassetsschools.org

audit mobile equipment.

- **Ransomware Attack:** Just as schools reopened in September 2021, criminals encrypted the District's computer systems with ransomware. This cyberattack on the District's computer network resulted in a massive disruption to the District's normal IT operations. The cyberattack impacted the classroom environment and strained IT staffing resources. It shifted our priorities as we were forced to deploy a team of IT professionals to methodically determine which of the District's systems were impacted. Our IT staff prioritized responding to the cyberattack and rebuilding the network server configurations.

As a District, we continuously strive to improve our practices, procedures, and methods to safeguard taxpayer funds appropriately. Steps have been taken to date regarding our investment in IT assets. Those steps, as well as additional steps we are planning to implement, will be delineated in the forthcoming corrective action plan to be submitted by our Board of Education. We appreciate your feedback and thank you for your recommendations. We take your findings and recommendations seriously as we endeavor to improve our processes in safeguarding our IT inventory.

Sincerely,

✓ Dr. Gaurav Passi
Superintendent of Schools

Cc: Manhasset Board of Education
Dr. Sean Adcroft

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 selected the District for audit from a list of school districts (excluding NYC schools) with enrollment greater than 300 and not currently in the OSC audit process at the time of selection. We classified school districts into four groups by enrollment and, using a random number generator, selected Districts from these groups. The list was broken out by geographic region for an even representation of school districts across the State for this multi-unit audit.
- We interviewed District officials and reviewed District policies and Board minutes to gain an understanding of IT asset management.
- We reviewed the District IT Department IT asset record provided by the District to determine if it contained sufficient information to identify IT assets.
- We selected a sample of 50 IT assets purchase from District invoices. Forty were from District invoices and 10 from student device reports. For 40 assets, we selected the largest invoice(s) from each IT vendor and selected IT assets over \$195. Ten student devices were selected based on a four-month school access inactivity report. We reviewed purchase orders, invoices, and/or packing slips and District inventory records to determine if assets were added to the inventory record and physically located in the District.
- We performed a walkthrough of District facilities and judgmentally selected 10 assets to determine whether the assets were accurately recorded on the inventory record. During our visual inspection of District IT assets, we assessed the general condition of their locations for the potential risk of damage or loss.

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

STATEWIDE AUDIT – 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.state.ny.us

