



Longwood Central School District

Review of Information Technology Inventory

For the 2021-2022 School Year

August 2022

The Board of Education
Longwood Central School District
35 Yaphank Middle Island Road
Middle Island, New York 11953

Board of Education:

We have been retained to function as the internal auditor for the Longwood Central School District (hereinafter, "the District"). Our responsibility is to assess internal control systems in place within the District, and to make recommendations to improve upon possible control weaknesses or deficiencies. In doing so, we hope to provide assurance to the District's Board, management, and residents that the fiscal operations of the District are being handled appropriately and effectively.

BACKGROUND

We assessed certain aspects of the District information technology (IT) environment and issued a report of our review in June 2013. Technology has shifted from the traditional desktop environment to handheld devices that permit users to perform similar functions without being constricted to one location. Such mobile computing devices (MCDs) include tablets, smartphones, personal digital assistants (PDAs), laptops, and netbooks. While such portability has facilitated employee productivity, expanded learning opportunities for students, and allowed for greater and faster communications, these devices can introduce security vulnerabilities.

PURPOSE

Due to COVID-19, school districts across the State had to cease in-person instruction in mid-March 2020. At that time, the District started distributing the available laptops to students and staff to enable them to operate remotely. The District's opening plan for the 2020-2021 school year necessitated continued remote learning; therefore, all students and staff needed appropriate devices to connect to the District. This included purchasing laptops, Chromebooks, and webcams/and projectors. The District utilizes a spreadsheet to track such inventory. As the District is in the process of implementing a 1:1 initiative whereby students in grades 5 and grades 9 received a Chromebook, and each year, the District will be purchasing more Chromebooks so that all students will eventually have a Chromebook. In addition, the District purchased approximately 312 Chromebooks that were purchased in part from a State grant.

In addition, New York State Education Law 2-d requires districts to ensure they protect students' personally identifiable information (PII) by ensuring that the use and disclosure of PII benefits students. It also prohibits the inclusion of PII in public reports or other public documents. This resulted in districts requiring a data privacy agreement with vendors that may obtain student PII.

The purpose of our review was to determine whether the internal controls are sufficient to ensure that IT equipment purchased as a result of the pandemic (i.e., Chromebooks, web cams, and

projectors), as well as software applications used are properly inventoried. In addition, our review assessed the adequacy of internal controls to comply with Ed Law 2-d.

SCOPE

The scope of this review entailed gaining an understanding of the internal controls to protect such devices and the information contained within them. This was accomplished by:

- Reviewing the current policies and procedures in place related to IT inventory as well as policies that address the risks of exposure of Personal Private and Sensitive Information (PPSI) and effectively protect computing resources to ensure compliance with Ed Law 2-d;
- Assessing the procedures for tracking and safeguarding computer equipment, including when equipment is transferred or deemed obsolete;
- Testing a sample of IT equipment to determine the completeness and accuracy of the District's inventory information; and
- Assessing the management and utilization of software applications and the process for ensuring compliance with Ed Law 2-d.

CONCLUSION:

The District is utilizing an IT inventory tracking system and is working to ensure the inventory records are accurate. While we noted internal controls have been implemented, we noted areas where controls could be improved. Sections I through III describe the results of our review and provide recommendations to improve the internal controls surrounding computer equipment and software application inventory controls in the District.

I. POLICIES & PROCEDURES

Good governance and accountability require the District's Board to adopt policies and procedures related to IT to provide criteria and guidance for the District's computer-related operations. To effectively protect computing resources and data, districts should have an acceptable use policy to inform users about appropriate and safe use of District computers, a hardware sanitization policy to ensure that equipment is not discarded with sensitive data and a breach notification policy in the event that sensitive data is compromised. These policies should be reviewed periodically and updated, as necessary, to reflect changes in technology or a district's computing environment. A district's Board is responsible for this review and update process.

Since devices have become more mobile, district officials are responsible for implementing policies and procedures that ensure the security of district MCDs. The NYS OSC has issued guidance that policies should also define which devices are covered (e.g., district-owned or personally-owned), and should indicate the "procedures for reporting lost or stolen MCDs and storage devices, the process used for gaining approval before connecting new devices to the system, and user responsibilities." Districts should have specific care and use guidelines for all district-owned MCDs that are given to staff/students and should require staff/students to sign an agreement regarding care and use of district-owned MCDs. Managing and tracking inventory has become even more important when the District had to implement a remote learning environment due to the pandemic, requiring all students and staff to have a device that can connect to the District.

The District has adopted several policies surrounding IT. These include:

- **Policy 4321.2: Confidentiality and Access to Individualized Education Programs and Individualized Education Services Programs**, which addresses the importance of ensuring confidentiality of personally identifiable data pertaining to student a student with a disability.
- **Policy 4526 and 4526.1: Acceptable Use of School District Computers and Internet Safety**, which addresses student internet access, addresses users who do not use the District's computers for educational purposes and indicates what constitutes appropriate and inappropriate use of IT equipment.
- **Policy 6800: Fixed Asset Accounting**, which states all equipment costing more than \$1,000 must be inventoried, and all computer hardware and mobile items should be inventoried for control purposes regardless of cost.
- **Policy 6900: Disposal of District Property**, which describes the process for properly disposing of school district assets.
- **Policy 8630 Computer Resources and Data Management and Policy 8630-R Computer Resources and Data Management Regulation**, which addresses district employees and third-party users who do not use the District's computers for instructional purposes, indicates what constitutes appropriate and inappropriate use of IT equipment and specifies the Boards expectations concerning the personal use of IT equipment or user privacy.
- **Policy 8635: Information Security Breach and Notification and Policy 8635-R Information Security Breach and Notification Regulation**, which detail how the District would notify an individual(s) whose private information was or is reasonably believed to have been compromised.

In addition, the District has implemented a process whereby students and teachers using a District Chromebook complete and sign an agreement outlining the responsibilities of the individual/family regarding the safekeeping of the device.

Issue #1: While the District does have formalized procedures on how IT devices should be utilized to safeguard technology resources (i.e., access security protocols), and has processes in place to sanitize hardware when being disposed, policy #6900 does not specify how the disposal of hardware equipment will ensure compliance with Ed Law 2-d, which requires the District to ensure that sensitive data is protected at all times.

Risk: Increased risk to unauthorized access to data that may contain personal and sensitive information.

Level: Moderate-High

Recommendation: We recommend that the District amend policy #6900 to describe how the District will ensure that all District-related data and information is permanently and completely removed. This should include if such data or information is of a sensitive, personal or confidential nature, and cannot be permanently and completely removed prior to discarding or selling, the equipment or supplies should be destroyed, and if reassigned or stored, the district should note that district data or information has not been permanently and completely removed. The district should also ensure that all

district-related data and information is permanently and completely removed from equipment that is leased from a third party, prior to returning the equipment.

II. IT PHYSICAL INVENTORY & ASSET MANAGEMENT

A detailed inventory record should include a description of each item, including make, model and serial number; the name of the person to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase information including acquisition date and cost. Each item also should be immediately affixed with an identification tag and entered into a consolidated inventory record upon receipt. Tracking all IT equipment helps to ensure that assets are properly secured and used for their intended purpose. In addition, a district can then determine the life cycle of such assets and be able to make decisions about future purchases.

The District maintains a spreadsheet to record and track the inventory of the IT equipment (e.g., Chromebooks, Smart Panels, document cameras, and webcams). To assess the adequacy, accuracy, and existence of the inventory maintained in the spreadsheet, we performed various tests as indicated below.

A. Onsite Inventory of IT Devices:

We selected a representative sample of 60 devices (5 Smart Panels, 8 All-in-Ones, 3 document cameras, 5 computers, 2 laptops, 37 PC's) from the District's inventory spreadsheet based on the type assigned to the device. We then verified whether the device was at the location as stated in the inventory system and verified whether the inventory records for that device (e.g., tag number, serial number, location, user, etc.) were accurate. In addition, we randomly selected 26 devices found at various school buildings throughout the District to verify whether the inventory records captured the asset's data and that the data captured is accurate.

Issue #2: We noted the following results from our testing:

Spreadsheet to Location test:

- There were 8 devices (6 PC's, 1 All-in-One, and 1 document camera) that were not found at the stated location per the spreadsheet.
- There were 2 Smart Panels where the serial number was not listed in the spreadsheet; however, we were able to confirm the existence of the devices based on the tag number, the model information, and the room number listed in the spreadsheet.
- There 3 All-in-One devices, 2 PC devices and 1 document camera where the tag number was missing from the spreadsheet. We were able to confirm the existence of the all the devices (except the document camera) based on the serial number, the model information, and the room number listed in the spreadsheet.
- There were 2 devices, 1 computer and 1 All-in-One, where the serial number on the device did not match the serial number in the spreadsheet (the last number/letter was incorrect); however, we were able to confirm the device the existence of the devices based on the tag number, the model information, and the room number listed in the spreadsheet.

Location to Spreadsheet test:

- There were 3 devices found at the High School, 1 PC and 2 computers, that were not listed in the inventory spreadsheet.
- There was 1 document camera whose tag number was not recorded in the inventory spreadsheet.
- There were 2 devices, 1 PC and 1 computer, whose serial number did not match the serial number listed on the inventory spreadsheet (the last number/letter was incorrect). All other information (asset tag number, model description, and location) were correctly entered.

Risk: The District may not be able to adequately safeguard and account for all IT assets, which may lead to unnecessary purchases, inaccurate budgeting, and loss of assets.

Level: Moderate-High

Recommendation: We recommend the District create formal procedures for documenting the inventory of IT devices within the inventory spreadsheet. In addition, although we understand that this may require the District to obtain additional resources, we recommend the District perform an inventory of IT assets on at least an annual basis. Our understanding is that the District recently implemented an IT asset management system. The implementation of such a system rather than a spreadsheet should help to facilitate performing the physical inventory of IT equipment.

B. **Assignment of Student Chromebooks:**

The Chromebooks are generally being used by students at the high school and the middle school. Staff at the high school and middle school building were responsible for distributing Chromebooks to students as well as maintaining the device agreement form. To assess the adequacy and accuracy of this spreadsheet, we selected forty (40) Chromebooks assigned to a student from the District's inventory spreadsheet (20 at the high school, 18 at the middle school, 1 at the junior high school, and 1 at Ridge elementary school), and then assessed whether the student was currently enrolled in the District and whether there was a signed agreement.

Issue #3: We noted the following:

- The buildings do not have standardized documented procedures for handing out and tracking Chromebooks provided to students.
- 1 student was assigned a Chromebook but was not an active student. The location of this device is unknown.
- 8 signed student device agreements could not be located.
- The device asset tag and serial numbers were not consistently documented on the student device agreement form. Without having the user sign an agreement for a specific device, the District would be unable to identify which device(s) and/or how many devices have been assigned to any specific student.
- The inventory spreadsheet lacked the asset tag number for 17 devices.

Risk: There is an increased risk that devices may be lost/stolen and not readily detected.

Level: Moderate-High

Recommendation: We understand that this is a relatively new process for the District. We recommend that the District develop a formal procedure so that buildings can ensure devices given to students are properly disseminated and tracked and are properly communicated to the IT department. This will entail ensuring the student agreement contains the asset tag and serial number of the device being provided. In addition, Chromebook Tracking using a Mobile Device Management software should be utilized to track the location of a Chromebook in the case of theft or misplacement. Lastly, the IT department, along with the building attendance staff, should develop procedures to ensure devices are returned when a student exits from the District, and should review the list of students with devices on a quarterly basis to ensure assigned devices are for active students only.

C. **Assignment of Faculty/Staff Devices:**

We selected 60 devices (Chromebooks) assigned to faculty/staff from the District's inventory spreadsheet. We then obtained the employee's name associated with the assignment to determine whether the device was being used by an active employee. Lastly, we obtained the last login date to assess whether if the device was being actively used. We noted that 46 of the 60 devices were assigned to a specific employee, and we confirmed all 46 devices were assigned to active employees of the District. Per discussions with the District, the remaining 14 devices were not assigned to an employee and were waiting to be deployed.

Issue #4: We noted the following:

- 36 of the 60 devices did not have a tag number entered in the inventory spreadsheet, thereby making it more difficult for the District to properly manage inventory.
- Of the 46 devices that were assigned to an employee, 7 devices had not been used for over two months, 4 of which had not been used in over 6 months. Devices that are not regularly used may be indicative that the device is not working properly or is lost/stolen.
- Of the 14 devices that were not assigned, 8 were used within a few weeks of our test period, which may indicate that the device is being used by an unauthorized user. In addition, we noted 6 devices were not used in over 5 months, 1 of which was not used in almost 3 years. The District was unable to confirm the location of these devices.

Risk: There is an increased risk that devices may be lost/stolen and not readily detected.

Level: Moderate-High

Recommendation: We recommend that the District perform a full inventory assessment of all Chromebook devices assigned to faculty/staff to ensure all devices are properly accounted for on an annual basis. The District should ensure all devices are properly tagged and that the tag numbers are recorded in the District's inventory spreadsheet. Lastly, we recommend that the District review the last date used at least annually (before

year-end) to determine whether there are any active devices that have not been used within a period of time before the report is run. The District would then investigate the existence of those devices to ensure the device has not been lost/stolen.

III. SOFTWARE APPLICATION INVENTORY MANAGEMENT

As per the District's Instructional Technology Plan 2022-2025, the District is committed to providing effective professional development sessions for its administrators, teachers, and staff to support the teaching and learning process. The District added four (4) full-time Instructional Coaches for Technology to support more classroom-embedded professional development (PD) for teachers, which included using various educational software applications. These sessions focused on the multi-dimensional needs of administrators, teachers, and staff, as well as being aligned with the District's overall goals to improve instruction and learning. To support PD, the district instructional technology applications were inventoried and aligned to the various educational content areas. After being presented with the District-provided instructional technology applications, and their alignment to curriculum, teachers in grades K-6 completed a survey on their knowledge and use of the District-provided instructional technology applications. In addition, Instructional Coaches for Technology meet frequently to collaborate on the integration of technology in content areas. This allows the District to assess the utilization associated for each software application and to ensure the costs are in line with District goals.

Ed Law 2-d requires NYS educational agencies to implement a multitude of regulations including:

- Developing and implementing a Data Security and Privacy Policy.
- Publishing a Parent's Bill of Rights as well as including it in every contract with a third-party contractor that receives PII.
- Mandating that all third-party contractors submit a Data Security and Privacy Plan for each contract to demonstrate how they will protect PII.
- Adopting the NIST Cybersecurity Framework as the standard for data privacy and security and meet the requirements to ensure they are adequately protecting PII.

District procedure is to ensure each software vendor has a Data Security and Privacy Plan which is disclosed in the District's Data Privacy Agreement signed by each vendor.

As part of our review, we obtained a listing from the District of software programs and selected 8 software applications. We reviewed each software vendor's Data Privacy Agreement, and usage data to determine whether the District is complying with Ed Law 2-d. **No exceptions were noted.**

Auditor's Comment: We noted one vendor who provided different wording on the District's Data Privacy Agreement. Any changes that are made to the document should be reviewed by the District's legal counsel to ensure the changes are appropriate and meet the District's data privacy needs. In addition, the District should date stamp when the agreements have been received so they can be properly tracked.

We would like to thank the staff at the District for its cooperation and professionalism during our testing.

We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures. Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,

Cerini & Associates LLP

Cerini & Associates, LLP
Internal Auditors