

OFFICE OF THE NEW YORK STATE COMPTROLLER



DIVISION OF LOCAL GOVERNMENT  
& SCHOOL ACCOUNTABILITY

# Protecting Personal, Private, and Sensitive Information When Disposing of or Reusing Electronic Equipment

2011-MS-2



Thomas P. DiNapoli

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	2
<b>EXECUTIVE SUMMARY</b>	3
<b>INTRODUCTION</b>	5
Background	5
Objective	7
Scope and Methodology	8
Comments of County, City, and School District Officials	8
<b>GUIDANCE FOR THE PROTECTION OF PPSI</b>	9
Written Policies	10
Written Procedures	12
PPSI Testing	13
Monitoring the Sanitization Process	15
Recommendations	16
<b>BREACH NOTIFICATION POLICY</b>	17
Recommendation	18
<b>APPENDIX A</b> Responses From Local Officials	19
<b>APPENDIX B</b> Audit Methodology and Standards	21
<b>APPENDIX C</b> Summary of Statistical Data for Audited Municipalities and School Districts	22
<b>APPENDIX D</b> How to Obtain Additional Copies of the Report	24
<b>APPENDIX E</b> Local Regional Office Listing	25

# State of New York Office of the State Comptroller

---

---

## **Division of Local Government and School Accountability**

February 2012

Dear Local Government and School District Officials:

A top priority of the Office of the State Comptroller is to help municipalities and school district officials manage resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support operations. The Comptroller oversees the fiscal affairs of local governments and school districts statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit, titled Protecting Personal, Private, and Sensitive Information When Disposing of or Reusing Electronic Equipment. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for local government and school district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller  
Division of Local Government  
and School Accountability*



## State of New York Office of the State Comptroller

---

# EXECUTIVE SUMMARY

Local governments and school districts all maintain records, both written and electronic, that potentially contain personal, private, and sensitive information (PPSI). To ensure sensitive personal and financial data is not accessible by unauthorized persons, local governments and school districts must make sure that electronic equipment is sanitized (that is, PPSI is entirely destroyed or removed from the equipment) prior to its disposal or reuse.

Local governments and school districts in New York State potentially store PPSI information in electronic form for more than 11 million<sup>1</sup> people. The eight entities included in this audit (Fulton, Oneida, Steuben, and Westchester Counties, the Cities of Port Jervis and Syracuse, and the Dansville and Shenendehowa Central School Districts) serve approximately 1.5 million people. Records of these entities indicated that they had disposed of 5,090 computers and related electronic equipment items, and 152 copiers, including 121 multi-function copiers with hard drives during our audit period.<sup>2</sup> All of this equipment potentially had the ability to store the PPSI of these entities' employees, students, and citizens.

### **Scope and Objective**

The objective of our audit was to determine whether these municipalities and school districts adequately protected PPSI when disposing of or reusing electronic equipment. Our audit addressed the following related questions:

- Do local officials have written policies and procedures for identifying the security risks of electronic data and for removing PPSI from equipment before its disposal or reuse?
- Do local officials have a breach notification policy in place?

### **Audit Results**

Only two of the eight entities, Fulton and Steuben Counties, had written policies covering the removal of PPSI from computers and related electronic equipment<sup>3</sup> before it is discarded or reused;

---

<sup>1</sup>These figures do not include the five counties of New York City, its one school district, or the City itself. <http://www1.osc.state.ny.us/transparency/LocalGov/LocalGovFaq.cfm#24>

<sup>2</sup>A multiple-function copier is a machine that combines the functions of many office devices into one to provide centralized document management. Common function combinations are printer, scanner, copier, and fax machine.

<sup>3</sup>These written policies did not cover copiers.

only one entity, Steuben County, had written procedures detailing the steps to take to protect PPSI on such equipment. At the start of our audit,<sup>4</sup> none of the entities had written procedures for removing PPSI from the hard drives of copiers before they are discarded. Further, none of the entities had implemented a written method of classifying the security risk of all the types of electronic data they store. When local governments and school districts lack written policies and procedures for identifying PPSI and for sanitizing equipment before disposal, there is an increased risk that PPSI could be obtained from discarded equipment and misused. Further, if local officials are not aware of the security requirements of all the data they maintain, they could potentially expose confidential data when they discard old equipment.

Our tests of 27 PDA-Smart phones did not find any PPSI on the devices, but examination of 65 computers prepared for disposal identified PPSI on five computers. Information included a child's health evaluation, bank account and tax lien data, and firewall information. Tests of 121 copiers with hard drives found that 55 of these copiers were disposed of with intact hard drives that likely contained PPSI. Exposing any of this data to unauthorized users could result in a breach of security. Steuben County was the only entity that had documented its sanitization efforts; however, this process did not cover copiers and did not require verification of employees' work. Unless local officials effectively monitor the sanitization of all types of discarded electronic equipment, confidential data on this equipment is vulnerable to misuse.

Finally, four entities had adopted breach notification policies, as required by statute, and one school district adopted such a policy as a good practice. Staff at three of these entities told us they did not know the steps to follow if a breach occurred. The other three entities had not developed a breach policy at all. Local officials should develop a breach notification policy and inform employees about it so their staff will be prepared to protect the public from persons who have obtained personal information without proper authorization.

### **Comments of County, City, and School District Officials**

The results of our audit and recommendations have been discussed with local government and school district officials and their comments, which appear in Appendix A, have been considered in preparing this report.

---

<sup>4</sup>Shenendehowa CSD documented its previously unwritten procedures for copier sanitization during audit fieldwork.

# Introduction

## Background

Regardless of their size or complexity, local governments and school districts all face similar information technology (IT) security risks. Securing technology equipment and electronic storage devices can prevent security breaches that can result in loss of individuals' personal, private, and sensitive information (PPSI). Such breaches can be very costly in financial terms, and can also result in lost productivity, lost confidence on the part of residents, and negative publicity.

PPSI is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or citizens of New York,<sup>5</sup> in general. Private information could include one or more of the following: Social Security number; driver's license number or non-driver ID; account number, credit card or debit card number and security code; or access code/password that permits access to an individual's financial account.

PPSI containing personally identifiable information might exist on hard drives, tapes, compact discs (CDs), digital video disks (DVDs), floppy disks, thumb drives, cell phones, multiple-function copiers, personal digital assistants (PDAs), or other storage devices, at times without the user's knowledge. Often electronic equipment stores sensitive data simply by viewing a computer file, which can create a copy of the file on the computer's hard drive; even when a user has deleted a file, it can still be retrieved using recovery software tools. When users purchase new electronic equipment, they often dispose of older items or sometimes reuse them. It is important to recognize that PPSI could still be stored on, and could be retrievable from, old electronic equipment.

This is not just a hypothetical risk. In an April 2010 media broadcast, media staff reported that they had been able to retrieve PPSI from four used copiers purchased from a New Jersey warehouse. Using free data recovery software available on the Internet, media staff recovered thousands of documents from the machines. Three copiers yielded the following: detailed domestic violence complaints and a list of wanted sex offenders; "targets" in a major drug raid; design plans for a building near Ground Zero in Manhattan; 95 pages of pay stubs with names, addresses,

<sup>5</sup><http://www.dhSES.ny.gov/ocs/resources/documents/Definitions-Acronyms.pdf>

and Social Security numbers; and \$40,000 in copied checks. The fourth machine, previously used by a health insurance company, contained 300 pages of individual medical records, including drug prescriptions, blood test results, and a cancer diagnosis. The company was required to notify more than 409,000 individuals that their personal or medical data may have been compromised.

Local governments and school districts use and maintain data in electronic form that contains PPSI. While a standard disposal policy informs staff how to dispose of electronic equipment (e.g., declaring surplus, allowing auction, selling on the internet, recycling, donating), a PPSI protection policy states the need to remove PPSI using a sanitization process upon disposal or transfer of such items. Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed. The three methods include wiping software programs, which overwrite random data onto the space where files are located; degaussing, or erasing information on the hard drive using a very strong magnet; and physical destruction, such as shearing, burning, crushing, or smashing. Table 1 shows some sanitization processes which are recommended for various types of electronic equipment per the Multi-State Information Sharing and Analysis Center.

**Table 1: Recommended Techniques for Disposal of Electronic Storage Media<sup>6</sup>**

Erasure and Disposal Technique Matrix					
Media Type	Wipe	OR	Degauss	OR	Physical Destruction
Computer Hard Drive Network Hard Drive External Drives	✓		✓		✓
Fax Machine Printer Copier	✓				✓
CDs DVDs					✓
USB Drives Thumb Drives Memory Sticks	✓				✓
Floppy Disks	✓		✓		✓
Tapes	✓		✓		✓
PDA's Cell Phones	✓				✓

<sup>6</sup>Local Government Cyber Security: Erasing Information and Disposal of Electronic Media (<http://www.msisac.org>)

We examined the relevant policies and procedures of eight municipalities and school districts in locations throughout New York State. Specifically, we audited four counties (Fulton, Oneida, Steuben, and Westchester), two cities (Port Jervis and Syracuse), and two school districts (Dansville and Shenendehowa) for the period January 1, 2008 through May 12, 2011.

A local municipality's governing board is generally responsible for the disposition of electronic equipment and the protection of PPSI stored on this equipment. In five of the eight entities we audited, the governing body has transferred the power to declare excess equipment surplus and/or authorize its sale or disposal to other individuals or departments within the municipality or school district. In four of these entities, the purchasing department was assigned this task, and the Chief Information Officer has been designated to surplus and dispose of electronic equipment in the fifth entity.

The local governments and school districts we audited serve approximately 1.5 million people and 11,540 students, respectively. Records show that these municipalities and school districts disposed of 5,090 computers (and related electronic equipment) and 152 copiers (121 of which were multi-function<sup>7</sup> copiers with hard drives) during our audit period. All of these electronic devices with memory potentially stored PPSI. See Table 3 in Appendix C for details about the size and the quantity of electronic equipment disposed of during the audit period.

## Objective

The objective of our audit was to determine whether these municipalities and school districts adequately protected PPSI when disposing of or reusing electronic equipment. Our audit addressed the following related questions:

- Do local officials have written policies and procedures for identifying the security risks of electronic data and for removing PPSI from equipment before its disposal or reuse?
- Do local officials have a breach notification policy in place?

---

<sup>7</sup>A multiple-function copier is a machine that combines the functions of many office devices into one to provide centralized document management. Common function combinations are printer, scanner, copier, and fax machine.

**Scope and Methodology**

For the period January 1, 2008 to May 12, 2011, we interviewed local government and school district officials and staff, and reviewed policies and procedures to identify the controls established. We also reviewed supporting documentation of equipment disposal, examined tracking and monitoring of sanitation efforts, and tested for the presence of PPSI on electronic equipment ready for disposal.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report.

**Comments of County, City, and School District Officials**

The results of our audit and recommendations have been discussed with local government and school district officials and their comments, which appear in Appendix A, have been considered in preparing this report.

## Guidance for the Protection of PPSI

As a matter of good practice, each municipality or school district that maintains a system of records should establish written procedures for the development, operation or maintenance of such a system; establish appropriate administrative, technical and physical safeguards to ensure security of records; and establish rules governing the retention and timely disposal of records. However, as shown in Table 2, we found that only Steuben and Fulton Counties had written policies for protecting PPSI before electronic equipment is discarded or reused, and that only Steuben County had written procedures detailing the steps employees must take to protect PPSI. At the start of the audit, none of the eight entities had written procedures for removing PPSI from the hard drives of copiers before they are disposed of. In addition, none of the entities had implemented a written method of classifying the security risk of all the types of electronic data they store. When local governments and school districts lack written policies and procedures for identifying PPSI and for sanitizing equipment before disposal, there is an increased risk that PPSI could be obtained from discarded equipment and misused. Further, if local officials are not aware of the security requirements of all the data they maintain, they could potentially expose confidential data when they discard old equipment.

Tests of 27 PDA-smart phones did not find PPSI on the devices, but tests of 65 computers prepared for disposal identified PPSI on five computers; tests of 121 copiers with hard drives found that 55 copiers were disposed of with intact hard drives that likely contained PPSI. Exposing any of this data to unauthorized users could result in a breach of security. Steuben County was the only entity that had a monitoring process to document its sanitization efforts; however, this process did not cover copiers and did not require verification of employees' work. Unless local officials effectively monitor the sanitization of all types of discarded electronic equipment, individuals' confidential data on this equipment is vulnerable to misuse.

Entity	PPSI Policies and Procedures			
	Written policy to protect PPSI on <u>all electronic equipment</u> ?	Written procedures to protect PPSI on <u>computers and related equipment</u> ?	Written <u>procedures</u> to protect PPSI on <u>copiers</u> ?	Data classification scheme to assign level of security risk?
Westchester County	No	No	No <sup>(a)</sup>	No
Oneida County	No	No	No <sup>(b)</sup>	No
Steuben County	Yes	Yes	No	No
Fulton County	Yes	No	No	Yes <sup>(c)</sup>
City of Syracuse	No	No	No	No
City of Port Jervis	No	No	No	No
Shenendehowa CSD	No	No <sup>(d)</sup>	Yes <sup>(e)</sup>	No
Dansville CSD	No	No	No	No
<b>Total</b>	Yes=2 No=6	Yes=1 No=7	Yes=1 No=7	Yes=1 No=7

(a) Contract with lessor does outline the procedure for the change of possession for hard drives.  
(b) Oneida County added a clause requiring removal of PPSI from electronic equipment, including computers, copiers, and PDA-phones to the County Surplus Policy on 11/12/10 while audit fieldwork was underway.  
(c) Classification scheme is part of Information Security Policy, but departments interviewed were not aware of it.  
(d) Shenendehowa CSD has written procedures only for sanitizing server equipment.  
(e) During fieldwork, department officials created written procedures for the disposal of copiers.

**Written Policies**

To help protect PPSI from disclosure to unauthorized users, local officials should develop a comprehensive written privacy policy that recognizes the need to secure PPSI before disposing of or reusing computers and electronic equipment, other types of electronic media, and copiers, and then communicate this policy to staff who handle sanitization work. To be effective in protecting privacy, such a policy should also require that officials classify information in a consistent manner to determine the level of security each type of data needs, and conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data they maintain.

We found that only two<sup>8</sup> of the eight units (Steuben and Fulton Counties) had written entity-wide policies that required the protection or removal of PPSI before disposing or reusing computers or related electronic equipment. These counties’ policies required that all data be made unrecoverable before computer equipment is disposed of.

<sup>8</sup>Shenendehowa CSD had a written departmental policy regarding protecting PPSI on servers before reuse or disposal.

- Steuben County had developed several media-specific policies that declared the need to protect PPSI before disposal, outlined the procedures to do so, and communicated this information to the staff we interviewed. Steuben County was also the only entity whose policies addressed the protection of PPSI on data transport and storage equipment, such as USB flash drives, external hard drives, and removable media (e.g., CDs and DVDs).
- Fulton County had a policy for protecting PPSI, but its policy did not specify a method staff should use to remove PPSI from equipment; further, few employees, including those within the County’s Information Services Department, were aware of the policy.

However, neither of these counties — nor any of the other entities we audited — had developed policies designed to verify that PPSI is removed from the hard drives of multi-function copiers before the units are disposed of or reused. Because copiers can retain PPSI in memory, it is essential that written privacy policies cover copiers as well as computers and other electronic equipment.

All information, whether in paper or electronic form, needs to be classified and labeled in a consistent manner to ensure data confidentiality, integrity, and availability. The data classification process assigns a level of risk to various types of information, which facilitates management’s ability to make appropriate decisions about the level of security the data requires. Entity officials should also conduct an inventory of PPSI stored on all types of electronic equipment the entity uses to ensure the data classification process is comprehensive.

We found that none of the eight units had implemented a written entity-wide data classification scheme. Fulton County had outlined the categories for a classification scheme in its IT Security Policy, but County officials had not put it into practice. None of the entities had conducted an overall inventory of PPSI stored on electronic equipment. If local officials do not classify the level of security risk associated with all the information they maintain in electronic form, and do not know where PPSI resides in all the electronic equipment they use, they risk exposing PPSI to unauthorized users when the equipment is disposed of or reused.

## Written Procedures

To support a PPSI protection policy, a municipality or school district should also have written procedures that outline the proper process to use to verify that PPSI is entirely destroyed or removed from electronic equipment prior to the equipment's disposal or reuse. Employees should be aware of the procedures and trained how to use them. We found that only Steuben County had written unit-wide procedures for removing PPSI from computers and related equipment.

At the other seven units,<sup>9</sup> department staff responsible for protecting the PPSI on computers at the point of disposal followed informal procedures. Table 4 in Appendix C details the disposal methods and sanitization processes used by all eight entities. In several of these entities, the unwritten procedures were complex enough to warrant being written to make sure staff understood the sanitization steps to take to protect PPSI on all types of equipment. For example, in Westchester County, the unwritten procedure for removing PPSI from a computer depended on the future disposition of the item: computers sold or donated for reuse had their hard drives sanitized with wiping software (which overwrites data on the hard drive) but those recycled had the hard drives removed and degaussed (erased). According to Shenendehowa CSD officials, staff used a sanitization procedure based on a computer's ability to access PPSI. For example, staff would wipe the hard drives of computers used by administrative staff before recycling the units. However, at both the above entities, there were no written procedures to help staff make these decisions. Written procedures with clear instructions for staff to follow help ensure that privileged information does not fall into the wrong hands.

All the municipalities and school districts we audited used one or more other kinds of electronic media that can store information, including PDAs, smart phones, USB flash drives, servers, external hard drives, and other removable media (CDs, DVDs and floppies). Steuben County is the only unit we examined that had written media-specific policies and written procedures for protecting PPSI before disposal or reuse for most types of electronic media. Some entities followed informal procedures for removing PPSI from specific equipment. For example, Oneida and Westchester Counties, the City of Syracuse, and Shenendehowa CSD provided selected employees with PDA-smart phones that could access municipal and district networks and save PPSI to memory. These entities' informal procedures called for wiping the

<sup>9</sup> Shenendehowa CSD also had written departmental procedures for removing PPSI from servers before reuse or disposal.

memory on the device before it was stored for reuse or disposal. No entity except for Steuben County tried to manage the use and disposal of small items like USB flash drives because they did not issue them or indicated that they could not effectively control the devices.

We also found that none of the eight entities had written, entity-wide procedures for removing PPSI from the hard drives inside of copiers. In fact, only three of the eight entities (Westchester County, City of Syracuse, and Shenendehowa CSD<sup>10</sup>) had even informal procedures to remove PPSI from copiers. Westchester County's practice involved formatting the hard drives or removing them for degaussing or physical destruction. The County then stored the hard drives in a secure area prior to recycling. Shenendehowa CSD purchased the copier hard drives for wiping at the end of the lease term. The City of Syracuse gave each department the choice of having the lessor return the hard drives for wiping, or having the lessor certify that it had performed the wiping function on returned copiers.

The other five entities had no procedure at all, meaning that their copiers were auctioned, sold through internet sales, returned to the lessor, recycled or sent to the landfill without regard to the leak of potential government, school district, or even individual PPSI to the next buyer, user, or finder. This uncontrolled disposal practice significantly increases the risk that unauthorized users could access and misuse confidential data without detection.

## **PPSI Testing**

Given the lack of written policies and procedures for protecting PPSI on computers and electronic equipment at most entities, and the absence of written policies and procedures to protect PPSI on copiers when we initiated our audit, we tested for evidence of PPSI on equipment that the eight entities disposed of during our scope period. We examined equipment or reviewed disposal records for a total of 244<sup>11</sup> items. Specifically, we examined 27 PDA-smart phones and 65 computers, and reviewed the records of all 152 copiers that the entities disposed of during this period, regardless of whether the copiers were returned to the lessor, auctioned, or recycled.

---

<sup>10</sup> During audit fieldwork, Shenendehowa CSD documented its process for sanitizing copiers.

<sup>11</sup> We selected our sampled items based on each entity's records (inventory, disposal, reuse, tracking, lease agreement) and physical observations for all equipment ready for disposal at the time of our audit test. We examined the equipment when it was still available or the records when the equipment (e.g., a leased copier) was no longer in the entity's possession.

Our tests of 27 PDA-smart phones did not identify PPSI on any of the units.

For the 65 computers, 45 computers should have had their hard drives wiped, and the remaining 20 computers should have had their hard drives removed, based on the entities' descriptions of the informal procedures they used. However, our tests showed that the hard drive on one of the 45 computers had not been wiped; we were able to view the contents of the hard drive using special software. Further, we found that the hard drives on four of the 20 computers were intact because we were able to start and run the computers. Therefore, five computers prepared for disposal — two computers at Oneida County and three computers in the City of Syracuse — had PPSI on their hard drives.

- In Oneida County, the computer whose hard drive was not wiped contained County Health Department user and administrator information and a child's health evaluation. Another computer from the County Sheriff's Department still had its hard drive intact, contrary to Department practice.
- In the City of Syracuse, the hard drives on three computers contained information that included bank account, tax liens, and firewall information.

Exposing any of this data to unauthorized users could result in a breach of security.

Our review of the records of 152 copiers showed that 31 copiers did not have hard drives, so they could not retain PPSI. For the 121 copiers with hard drives, records for 66 copiers showed that the hard drives were removed for destruction or contained lessor certifications that the lessor had wiped the hard drives. However, records for the remaining 55 copiers indicated that the units were disposed of with their hard drives intact. Disposal records showed that these machines had been sold (auctions or internet sales) or returned to the lessor. Because the hard drives were still in these units, it is likely that they all contained PPSI that could be retrieved and misused by unauthorized persons.

When local governments and school districts lack written policies and procedures for identifying PPSI on each media type and sanitizing equipment before disposal, there is an increased

risk that unauthorized users could obtain and misuse PPSI from discarded equipment. Such breaches can result in legal costs, embarrassment, and additional costs associated with notifications of information breaches.

### **Monitoring the Sanitization Process**

It is critical that a local government or school district maintain a record of electronic equipment disposals to document what media was sanitized, when, and how it was sanitized. The record should also document the final disposition date of the media. Inadequate recordkeeping of media sanitization can result in a loss of control over information that should be protected.

An essential step in maintaining reliable records is assigning personnel independent of the sanitization process to verify that PPSI is removed from electronic equipment. These personnel should test a sample of media from the inventory of equipment designated for disposal and document the results of their tests. The official responsible for protecting PPSI should document the completion of the media sanitization process to ensure that equipment has been properly sanitized and to establish proper accountability for inventory control purposes.

Steuben County was the only entity<sup>12</sup> that documented the process it used to remove PPSI from all electronic equipment, except copiers. The County had a standard sanitization practice that included using a work log to track the removal of PPSI from computer and related equipment before reuse or disposal. However, the County did not verify that staff actually wiped the equipment or filled out the tracking sheets accurately. In Westchester County, the lessor and County staff both signed a form showing when copier hard drives passed from one to the other, but the process did not document the destruction of the hard drive or monitor whether destruction was complete. Unless local government and school district officials maintain adequate records of the destruction of PPSI on equipment before it is disposed of, and monitor the effective sanitization of the equipment, they risk losing control over the status of confidential data.

---

<sup>12</sup>Fulton County writes the date and the word “wiped” on the computer shell for computers that will be auctioned. However, there is no written documentation supporting the removal of PPSI or monitoring that the procedure is being followed.

## **Recommendations**

1. Officials should establish written policies to ensure that all PPSI on electronic equipment (computers, related equipment and copiers) is removed prior to reuse and disposal.
2. Officials should develop written procedures that outline the proper process to use to ensure PPSI is entirely destroyed or removed from electronic equipment prior to disposal or reuse.
3. Officials should establish a data classification scheme.
4. Officials should account for all equipment that may contain PPSI, track the removal of the PPSI from the equipment prior to disposal and monitor compliance of the process by documenting the procedures.
5. Officials should coordinate with lessors, as necessary, to ensure that returned copiers are sanitized, and should document the completion of the sanitization process in accordance with entity-wide procedures for protecting PPSI in electronic equipment.

## Breach Notification Policy

State Technology Law Section 208 (Law) specifically states: “‘Breach of the security of the system’ shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity.”

This Law requires that State entities must disclose to a New York resident when their private information was, or is reasonably believed to have been, acquired by a person without valid authorization. Municipalities and other local agencies are required to have adopted a notification policy or local law consistent with the Law no later than April 6, 2006. Although it is unclear whether school districts are required by statute to adopt a notification policy, doing so is a good practice. When a breach occurs, notification of the breach should be made in the most expedient time possible without unreasonable delay, after necessary measures to determine the scope of the breach, restore integrity, and any delay if law enforcement determines that notification impedes a criminal investigation.

If local governments and school districts do not follow proper control procedures when disposing of electronic equipment, they may be compromising PPSI, and risking a breach event that could jeopardize personal privacy and result in identity theft. To comply with the Law, where applicable and to protect PPSI, municipalities and school districts should establish a breach notification policy, notify and train employees of the policy requirements should computer security breaches involve PPSI, and regularly audit compliance with the policy.

We found that Steuben and Westchester Counties had breach notification policies in place. Fulton County, the City of Port Jervis and Shenendehowa CSD<sup>13</sup> also had policies in place, but staff at these entities told us they were unaware of the policy and of the steps that needed to be taken if a breach event occurs. The remaining three entities, Dansville CSD, Oneida County, and the City of Syracuse, did not adopt a breach notification policy or local law.

---

<sup>13</sup>After the completion of fieldwork, District officials provided documentation supporting a new annual staff notification process to ensure staff are aware of the District’s breach notification policy.

A breach notification policy is an important tool that provides guidance for staff to follow during a breach event. Municipalities that lack a breach notification policy are not in compliance with the Law; for all entities, the lack of such a policy potentially delays the communication of compromised information to the necessary parties involved. Additionally, employees' lack of knowledge about the adopted policy could seriously jeopardize the effectiveness of the actions entities take to protect the public from persons who have obtained personal information without proper authorization.

**Recommendation**

6. Officials should establish a breach notification policy, notify and train employees and regularly audit compliance with the plan.

## APPENDIX A

### RESPONSES FROM LOCAL OFFICIALS

We provided a draft copy of this global report to each of the eight municipalities and school districts we audited and requested responses. We received response letters from six of the entities.

Overall, entity officials were in agreement with the findings and recommendations in the report. The following comments were excerpted from the responses we received.

#### Overall Comments

##### City of Syracuse

“Your report, along with its recommendations, provided us with a framework to make improvements to the City’s existing policies and procedures, including establishing a breach notification policy.”

“Similar to most of the other government entities reviewed in the PPSI audit, the City of Syracuse lacked written policies and procedures for both computers and copiers.”

##### City of Port Jervis

“The City has and will continue to improve its processes regarding the security of personal information in all forms. We have implemented some new procedures and will continue to assess exposures as new technology develops.”

##### Westchester County

“Westchester County understands and accepts the audit’s primary finding that formal documentation and control procedures would further enhance the organization’s ability to protect PPSI.”

“...the county is developing a comprehensive privacy policy and formal guidelines for the identification, protection and management of PPSI that will be applicable to all County employees and relevant third party contractors. The county is basing its policy on established PPSI guidelines and policy recommendations made by the Department of Homeland Security (DHS) in its highly regarded *Handbook for Safeguarding Sensitive Personally Identifiable Information*.”

##### Steuben County

“Steuben County has utilized your recommendations and revised its Administrative Code to specifically address sanitization of copy and fax machines hard drives, along with documentation of the monitoring process.”

“The report clearly demonstrates Steuben County’s commitment to information security and our implementation of strict policies and procedures for sanitization and disposal of equipment.”

## **Shenendehowa CSD**

“The district’s due diligence in the protection of data is ongoing and the recommendations provided will be used to improve upon those practices and the communications to staff.”

## **Oneida County**

“This has been a productive and educational process for Oneida County.”

“In addition to establishing clearly written policies and procedures recommended in your report, Oneida County will establish the two additional critical items identified in your report. First, for the purposes of clarifying any and all definitions of what constitutes PPSI data, Oneida County will institute a data classification scheme. Complimenting this scheme, we will also account for all equipment that may contain PPSI, and will create a countywide breach notification policy should there be a situation where a breach may occur.”

## APPENDIX B

### AUDIT METHODOLOGY AND STANDARDS

We judgmentally selected eight municipalities and school districts of varying sizes throughout the State, as determined by population or enrollment. We reviewed the policies and procedures of the local governments and school districts to gain an understanding of the controls in place and to determine if the controls provide proper security to protect PPSI when disposing of electronic equipment. We also reviewed inventory, disposal, reuse, tracking, and lease agreement records to identify items for testing.

We reviewed available records and made physical observations to identify items intended for sale and tested these items to determine if processes are adequate to protect PPSI. We used both the written and unwritten procedures as explained by entity staff as well as good business practices as criteria to determine testing result compliance. Computer equipment ready for disposal was tested to determine if PPSI was present and retrievable from the hard drives. If hard drives were not removed, we assessed them using specialized equipment to determine if they contained data that had not been overwritten. If the process used by the entity was the removal of the hard drive from the electronic device prior to disposal, our testing of computer equipment included opening the computer to verify that the hard drive had been removed according to the policy.

From a list of computers that were transferred or reused within the municipality or district, we selected items that were: 1) transferred from a department likely to have PPSI stored on computers; and 2) transferred outside of the original department. We found each of the selected computers and verified asset tag number, serial number, description and receiving department. We tested each computer to determine if it was reformatted as described by the entity's procedure or if it contained PPSI prior to the sanitization process.

We reviewed copier inventory and disposal lists to identify equipment disposed of during the scope period, and reviewed documentation regarding all returned or sold copiers, including lessor certification indicating whether the model had hard drives and the ability to store data. In one entity, a lessor representative stated that data was not stored on copiers that are not networked, so testing was conducted on a currently in-use non-networked multiple-function copier. The hard drive was examined using specialized equipment to determine if it contained data.

When applicable, we also reviewed inventory and disposal lists for PDA-smart phones and other related equipment. In four entities that issue PDA-smart phone devices, we examined the items waiting to be reused or disposed of, viewing all of the features to determine if data remained on the equipment.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## APPENDIX C

### SUMMARY OF STATISTICAL DATA FOR AUDITED MUNICIPALITIES AND SCHOOL DISTRICTS

<b>Table 3: Summary of Statistical Data for Audited Municipalities and School Districts (Sorted by Government Type and Size)</b>				
<b>Entity Name</b>	<b>Population (2010 U.S. Census) or Pupil Enrollment (2010-11)</b>	<b>Number of Computer and Related Equipment Disposals</b>	<b>Number of Copier Disposals (including copiers with and without hard drives)</b>	<b>Number of Copiers with Hard Drives</b>
Westchester County	949, 113	2,856	38	38
Oneida County	234,878	225	15	15
Steuben County	98,990	416	29	4
Fulton County	55,531	135	9	3
City of Syracuse	145,170	172	29	29
City of Port Jervis	8,828	2	0	0
<b>Subtotal</b>	<b>1,492,510</b>	<b>3,806</b>	<b>120</b>	<b>89</b>
Shenendehowa Central School District	9,800	953	30	30
Dansville Central School District	1,740	331	2	2
<b>Subtotal</b>	<b>11,540</b>	<b>1,284</b>	<b>32</b>	<b>32</b>
<b>Total</b>	<b>1,504,050</b>	<b>5,090</b>	<b>152</b>	<b>121</b>

<b>Table 4: Disposal Methods and Sanitization Procedures Used by the Eight Entities</b>			
<b>Entity Name</b>	<b>Disposal Method</b>	<b>Sanitization Process (Computer Equipment)</b>	<b>Sanitization Process (Multiple-Function Copiers)</b>
Westchester County	Internet Sales Company	Reformatting, wiping, degaussing, physical destruction	Degaussing and physical destruction
	Recycling		
	Donation		
Oneida County	Internet Sales Company	Reformatting, wiping, physical destruction, removal and securing of hard drives	None
	Recycling		
	Secure Storage		
Steuben County	Auction	Wiping, physical destruction and reimage	None
	Recycling		
Fulton County	Auction	Wiping, physical destruction	None
	Donation		
	Recycling		
City of Syracuse	Recycling	Physical destruction, degaussing, wiping and reformatting	Wiping, degaussing and physical destruction
Dansville CSD	Recycling	Wiping, reformatting, physical destruction	None
City of Port Jervis	Recycling	Formatting, removal and securing of hard drives	None
	Secure Storage		
Shenendehowa CSD	Recycling	Wiping and reimage <sup>(a)</sup>	Wiping and physical destruction

<sup>(a)</sup> Imaging a computer, also referred to as ghosting, is a process in which the computer is sanitized and restored to a common state with common programs.

## APPENDIX D

### HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller  
Public Information Office  
110 State Street, 15th Floor  
Albany, New York 12236  
(518) 474-4015  
<http://www.osc.state.ny.us/localgov/>

**APPENDIX E**  
**OFFICE OF THE STATE COMPTROLLER**  
**DIVISION OF LOCAL GOVERNMENT**  
**AND SCHOOL ACCOUNTABILITY**

Steven J. Hancox, Deputy Comptroller  
Nathalie N. Carey, Assistant Comptroller

**LOCAL REGIONAL OFFICE LISTING**

---

**BINGHAMTON REGIONAL OFFICE**

H. Todd Eames, Chief Examiner  
Office of the State Comptroller  
State Office Building - Suite 1702  
44 Hawley Street  
Binghamton, New York 13901-4417  
(607) 721-8306 Fax (607) 721-8313  
Email: [Muni-Binghamton@osc.state.ny.us](mailto:Muni-Binghamton@osc.state.ny.us)

Serving: Broome, Chenango, Cortland, Delaware,  
Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

**BUFFALO REGIONAL OFFICE**

Robert Meller, Chief Examiner  
Office of the State Comptroller  
295 Main Street, Suite 1032  
Buffalo, New York 14203-2510  
(716) 847-3647 Fax (716) 847-3643  
Email: [Muni-Bufferalo@osc.state.ny.us](mailto:Muni-Bufferalo@osc.state.ny.us)

Serving: Allegany, Cattaraugus, Chautauqua, Erie,  
Genesee, Niagara, Orleans, Wyoming Counties

**GLENS FALLS REGIONAL OFFICE**

Jeffrey P. Leonard, Chief Examiner  
Office of the State Comptroller  
One Broad Street Plaza  
Glens Falls, New York 12801-4396  
(518) 793-0057 Fax (518) 793-5797  
Email: [Muni-GlensFalls@osc.state.ny.us](mailto:Muni-GlensFalls@osc.state.ny.us)

Serving: Albany, Clinton, Essex, Franklin,  
Fulton, Hamilton, Montgomery, Rensselaer,  
Saratoga, Schenectady, Warren, Washington Counties

**HAUPPAUGE REGIONAL OFFICE**

Ira McCracken, Chief Examiner  
Office of the State Comptroller  
NYS Office Building, Room 3A10  
Veterans Memorial Highway  
Hauppauge, New York 11788-5533  
(631) 952-6534 Fax (631) 952-6530  
Email: [Muni-Hauppauge@osc.state.ny.us](mailto:Muni-Hauppauge@osc.state.ny.us)

Serving: Nassau and Suffolk Counties

**NEWBURGH REGIONAL OFFICE**

Christopher Ellis, Chief Examiner  
Office of the State Comptroller  
33 Airport Center Drive, Suite 103  
New Windsor, New York 12553-4725  
(845) 567-0858 Fax (845) 567-0080  
Email: [Muni-Newburgh@osc.state.ny.us](mailto:Muni-Newburgh@osc.state.ny.us)

Serving: Columbia, Dutchess, Greene, Orange,  
Putnam, Rockland, Ulster, Westchester Counties

**ROCHESTER REGIONAL OFFICE**

Edward V. Grant, Jr., Chief Examiner  
Office of the State Comptroller  
The Powers Building  
16 West Main Street – Suite 522  
Rochester, New York 14614-1608  
(585) 454-2460 Fax (585) 454-3545  
Email: [Muni-Rochester@osc.state.ny.us](mailto:Muni-Rochester@osc.state.ny.us)

Serving: Cayuga, Chemung, Livingston, Monroe,  
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

**SYRACUSE REGIONAL OFFICE**

Rebecca Wilcox, Chief Examiner  
Office of the State Comptroller  
State Office Building, Room 409  
333 E. Washington Street  
Syracuse, New York 13202-1428  
(315) 428-4192 Fax (315) 426-2119  
Email: [Muni-Syracuse@osc.state.ny.us](mailto:Muni-Syracuse@osc.state.ny.us)

Serving: Herkimer, Jefferson, Lewis, Madison,  
Oneida, Onondaga, Oswego, St. Lawrence Counties

**STATEWIDE AND REGIONAL PROJECTS**

Ann C. Singer, Chief Examiner  
State Office Building - Suite 1702  
44 Hawley Street  
Binghamton, New York 13901-4417  
(607) 721-8306 Fax (607) 721-8313