Westchester County Information Technology Policy	**No:** WC-P16-001
IT Policy: **Policy & Guidelines for Safeguarding Sensitive Personally Identifiable Information (PII)**	**Updated:** 01/12/2023
	Issued By: Westchester County Department of Information Technology (DoIT)
	Owner: Marguerite Beirne Chief Information Officer mcb1@westchestergov.com

1. Purpose

Westchester County, as a government entity, conducts public business. As such, the records related to the business of the County are generally available for public review. Nevertheless, Westchester County is committed, to the extent allowable by law, to safeguard Sensitive Personally Identifiable Information (PII). This privacy commitment must be balanced with the rights of public access under the Freedom of Information Law (FOIL) and consistent with any other applicable federal, state and local statute or regulation.

This policy is designed to also serve as a handbook that sets minimum standards for how all employees should handle Sensitive PII at Westchester County. This policy also covers any other individuals, including consultants, interns, temporaries and vendors, who have access to County technology facilities, computers or networks.

This document provides step-by-step guidance on how to identify and protect Sensitive PII:

- In the office or an alternate worksite
- On a portable device, such as blackberry or laptop
- When sent by email, fax, or other electronic transfer
- When sent by mail: external, overseas and inter-office

- When stored on a shared drive
- When you are on official travel

The policy also provides simple instructions on:

- Encrypting Sensitive PII
- Securing Sensitive PII when it is not in use
- Disposing of Sensitive PII

This policy is intended to help you safeguard Sensitive PII in paper and electronic form during your everyday work activities. By observing these guidelines, you will be doing your part to protect the Sensitive PII of our employees, contractors, and the public, by reducing the risk that a serious data breach will occur at Westchester County.

2. Authority

The Charter and Administrative Code of Westchester County, NY provides the Department of Information Technology (DoIT) with the authority to establish countywide technology policies, including technology and security standards. The County's Chief Information Officer has the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for County government, including hardware, software, security and business re-engineering.

3. Scope/Responsibilities

This policy covers all employees of Westchester County. It also covers any other individuals, including consultants, interns, temporaries and vendors, who have access to County technology facilities, computers or networks.

All individuals – as defined above – are responsible for complying with this policy and for immediately reporting any known or suspected violations of this policy to their immediate supervisor or the Department of Information Technology. The CIO must approve any exceptions to this policy. Requests for exceptions and the CIO's decision must be in writing and come from the appropriate Commissioner or Department Head.

4. What is Sensitive PII?

Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII, when maintained by Westchester County, are sensitive as

stand-alone data elements. Examples of such Sensitive PII include: Social Security number (SSN) and biometric identifiers. Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of employee names with poor performance ratings.

Not all PII is sensitive. For example, information on a business card or in a public phone directory of agency employees is PII, but in most cases not Sensitive PII, because it is usually widely available public information.

PII that is available to the public or that resides on test and development environments is still considered Sensitive PII in certain circumstances. For example, an individual's SSN might be available in a public record maintained by a local court; however, Westchester County would still consider that individual's SSN to be Sensitive PII because SSNs are a key identifier used in identity theft and therefore are inherently sensitive. As another example, a Westchester County employee might maintain a public website identifying him or herself as having a certain medical condition; however, that same medical information in that employee's personnel file at Westchester County would still be considered Sensitive PII.

PII That Is Always Sensitive

The following personal identifiers, when maintained by Westchester County, are Sensitive PII even if they are not coupled with additional PII or contextual information:

- complete (9-digit) SSN
- biometric identifiers (e.g., fingerprint, iris scan, voice print)

The following information is Sensitive PII when grouped with the person's name or other unique identifier, such as address or phone number:

- citizenship or immigration status
- medical information
- driver's license number
- passport number
- full date of birth
- authentication information such as mother's maiden name or passwords
- portions of SSNs such as last four digits
- financial information such as account numbers
- other data created by Westchester County to identify or authenticate an individual's identity

PII That Is Sensitive In Certain Contexts

Context matters. PII that might not include the data elements identified in 2.1 might still be sensitive and require special handling if it could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual.

For example, a collection of names is not Sensitive PII if it is a list, file, query result, etc. of

- attendees at a public meeting
- stakeholders who subscribe to a Westchester County listserv
- employees and contractors at the Department of Information Technology However, a collection of names IS Sensitive PII if it is a list, file, or query result of
- law enforcement personnel, such as investigators, agents, and support personnel
- employees with poor performance ratings

5. How to Safeguard Sensitive PII

You should exercise due care when handling all PII and all information you encounter in the course of your work for Westchester County. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised. The following handling guidelines apply to everyone working for or on behalf of Westchester County and explain how you must handle Sensitive PII at Westchester County.

Collect Sensitive PII Only As Authorized

Be sure that when you collect or maintain Sensitive PII, you have the legal authority to do so.

When collecting Sensitive PII from members of the public, do not create unapproved paper or electronic forms or processes to collect Sensitive PII.

Collecting personal data from members of the public may trigger separate legal requirements.

Limit Use of Sensitive PII

Only access Sensitive PII when you need to know that information, that is, when your need for the information relates to your official duties.

- If you work for Westchester County as a contractor, you must have a nondisclosure agreement (NDA) on file prior to handling Sensitive PII.
- Do not access or share Sensitive PII for entertainment or any other purpose unless it is related to your job function or need to know the information to perform your official duties.
- Remember that you must secure Sensitive PII in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.

Only use Sensitive PII for official purposes.

- If you are unsure about whether a specific use is appropriate, you should confirm with your supervisor.
- Do not browse files containing Sensitive PII out of curiosity or for personal reasons.

Share Sensitive PII only as authorized.

- You are authorized to share Sensitive PII with another Westchester County employee or contractor if the recipient's need for the information is related to his or her official duties.
- Refer requests for Sensitive PII from members of the public, the media, or other outside entities to your FOIL Officer.

Minimize Proliferation of PII

Do not create unnecessary or duplicative collections of Sensitive PII, such as duplicate, ancillary, "shadow," or "under the radar" files. Minimizing proliferation of Sensitive PII helps to keep it more secure and reduces the risk of a data breach.

- If you need to create duplicate copies of Sensitive PII to perform a particular task or project, delete or destroy them when they are no longer needed.

When you need to print, copy, or extract Sensitive PII from a larger dataset, target your actions to obtain data on only the specific individuals and the specific data elements you need to perform the task at hand.

Follow retention and disposal policies.

- The retention of Sensitive PII extracted from a system is not to extend beyond the records retention schedule or as identified in Executive Order No. 5 of 2008 on the Proper Management, Retention and Disposition of County Records (see section 7 below).
- Use appropriate destruction techniques to dispose of Sensitive PII.

    - Shred (do not recycle) papers containing Sensitive PII.
    - Computer drives and other electronic storage devices should be wiped of Sensitive PII before they are re-issued for use.
- Until you dispose of Sensitive PII, keep it secured in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.

Secure Sensitive PII

When you handle, process, transmit, and/or store Sensitive PII, you should limit the potential for unauthorized disclosure. To do this, protect against "shoulder surfing," eavesdropping, or overhearing by anyone without a need to know the Sensitive PII.

Sensitive PII may be saved, stored, or hosted only on Government equipment (including contractor-owned equipment or system that is approved to be used as a Government system.) Note that these rules also apply to individuals participating in approved Telework programs.

Do not take Sensitive PII home or to any non-County approved worksite, in either paper or electronic format, unless appropriately secured. Sensitive PII in electronic form must be encrypted. Paper documents must be under the control of the employee or locked in a secure container when not in use. Personally owned computers may not be used to save, store, or host Sensitive PII.

Physically secure sensitive PII (e.g., in a locked drawer, cabinet, or desk; in a safe; or in another locked container) when not in use or not otherwise under the control of a person with a need to know. Sensitive PII may be stored in a space where access control measures are employed to prevent unauthorized access by members of the public or other persons without a need to know (e.g., a locked room or floor, or other space where access is controlled by a guard, cipher lock, or card reader), but the use of such measures is not a substitute for physically securing sensitive PII in a locked container when not in use.

When you are emailing Sensitive PII outside of Westchester County, you must send the Sensitive PII within an encrypted attachment.

Do not leave Sensitive PII unattended on a desk, network printer, fax machine, or copier. Do not send Sensitive PII to a fax machine without contacting the recipient to arrange for its receipt.

Store Sensitive PII in shared access computer drives ("shared drives") only if access is restricted to those with a need to know by permissions settings or passwords.

Sensitive PII stored in such drives and associated permissions should be

reviewed on a periodic basis to ensure security.

Physically secure Sensitive PII when in transit. Do not mail or courier Sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted. Do not return failed hard drives to vendor for warranty if the device was ever used to store Sensitive PII, but sanitize or destroy the media. For example, do not pack laptops or electronic storage devices in checked baggage. Do not leave them in a car overnight or in plain sight in a parking lot.

If someone sends you Sensitive PII in an unprotected manner, you still must secure it once you receive it. If you receive a request to accept Sensitive PII in an encrypted format, you must be able to accept the Sensitive PII in that format so that the sender may comply with his or her requirements to encrypt Sensitive PII.

6. What Must You Do If You Suspect an Incident?

Westchester County defines a privacy incident as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users and for an unauthorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both suspected and confirmed incidents, whether intentional or inadvertent, involving PII which raise a reasonable risk of harm.

Westchester County has established a Security Breach Notification Policy which requires the County to take reasonable technological measures to protect its computerized data, and to notify the public when the possibility of an unauthorized acquisition or dissemination of their personal information may occur as a result of a security breach of the County's computer system or database. The Executive Order can be accessed in its entirety here: http://cww.westchestergov.com/executiveOrders/2006/012006.htm.

If at any point you suspect or know that Sensitive PII has been handled in a way that violates this policy, or otherwise suspect or know of a privacy incident at Westchester County, regardless of the reason or severity of the incident, you must:

Report Privacy Incident to Your Supervisor as Soon as It Is Suspected or Confirmed

Supervisors must report the incident to Chief Information Officer.

Document or maintain records of information and actions relevant to the incident, as it may be required in the privacy incident handling report.

Any alleged violations that may constitute criminal misconduct, identity theft or other serious misconduct, or reflect systematic violations will be reported to appropriate supervisors and the Chief Information Officer (CIO) as part of the privacy incident reporting process.

In addition, Westchester County is required to follow the security breach notification procedures as outlined in New York State Technology Law 208 as well as those included in Executive Order No. 1 of 2006, as referenced above.

Do Not Further Compromise the Information

Beware of these common mistakes so that your response to a privacy incident does not constitute another incident:

- Do not forward compromised information (e.g., SSN, full name, birth date, etc.) when reporting an incident.
- If and when the compromised Sensitive PII is needed by your supervisor, or the Helpdesk in order to respond to an incident, you will be given instructions on whether the compromised information needs to be forwarded to someone at Westchester County.
- If you see Sensitive PII in an email that you suspect constitutes a privacy incident, remember that the information is duplicated and further compromised if you forward it, reply, or "reply to all."
- Before you reply or forward an email, make sure that you remove any Sensitive PII that should not be disclosed from the email chain below.
- Be careful when "hiding" columns in spreadsheets that contain Sensitive PII. When emailed to a recipient who is not aware that a spreadsheet contains hidden columns, that person may inadvertently forward that spreadsheet to someone who does not need to know that information.

7. Monitoring & Privacy of Communications

Westchester County maintains the right to access and examine County computer systems and networks and all information that is stored or transmitted through these systems and networks, including all e-mail and website visits. All electronic communications are considered County records. As County records, electronic communications are subject to disclosure to law enforcement or government officials or to other third parties through FOIL (Freedom of Information Law) requests or other discovery process. Employees must ensure that information contained in electronic communications is accurate, appropriate and lawful.

While Westchester County does not intend to regularly review employees' e-mail

records, employees have no right or expectation of privacy in e-mail. Since the County is responsible for the servicing and protecting of its electronic communications networks and administering this policy, it is occasionally necessary to intercept or disclose electronic communication. Upon an employee's termination, the Legal Department, Human Resources or the employee's manager will direct his/her e-mail to be managed by another employee.

Communications on these Systems are not private. Users should be aware that the data they create on the System remains the property of the County, and usually can be recovered even though deleted by the user. Despite security precautions, there is no absolutely fail-safe way to prevent an unauthorized user from accessing stored files. The confidentiality of any information stored or transmitted on the System cannot be guaranteed. Furthermore, information that is stored on the System or sent via e-mail may be subject to disclosure pursuant to the New York State Freedom of Information Law and discovery.

8. Removable Media & Encryption

To minimize the risk of loss or exposure of Sensitive Personally Identifiable Information (PII) maintained by Westchester County and to reduce the risks associated with exposing the County to malware infections, virus attacks, system compromise, interruption of services and legal issues, the County has established an encryption policy that applies to removable media (any device that is capable of storing data that is readily portable and easily removed from the primary computer or other storage device).

This policy applies to all Westchester County employees and other individuals with access to the County network and provides specific guidelines for encrypting information stored on removable media, thereby preventing Sensitive PII from being intercepted by unintended recipients.

In addition, Westchester County does encrypt credit card data received via various e-commerce applications. The County also encrypts PC laptop drives to prevent third parties from accessing the PC should the device become lost or stolen. Electronic communications systems are, however, not routinely encrypted on a countywide basis. Employees must be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed and stored by others.

9. Management, Retention & Disposition of Records

Under the guidance of the Chief Information Officer (CIO), all departments and agencies of County government are responsible for the proper management, retention and disposition of their records.

Please refer to Executive Order No. 5 of 2008 on the Proper Management, Retention and Disposition of County Records for complete details regarding statutory and regulatory requirements, and further recommendations on how to comply. The Executive Order can be found on the County's intranet site under Office of the CE → Executive Orders or by clicking here: http://cww.westchestergov.com/executiveOrders/2008/exec_order_5_001.PDF.

10. Physical Security

Employees entrusted with Westchester County computer assets, including desktops, laptops and software, must exercise due diligence at all times to prevent theft, destruction or other misuse of the assets. Portable laptops, notebooks, smartphones, and other transportable computers containing sensitive County information must be treated with the same care provided to company documents.

11. Preventing Identity Theft and Data Loss

There are several steps that must be taken to reduce the possibility that confidential personal information in County hands will end up in the hands of identity thieves, including, but not limited to:

- Not moving County data to non-County equipment or unauthorized external, third-party hosting services (e.g., Dropbox, Google Drive, etc.) without prior written approval from the Commissioner and Chief Information Officer.
- Not copying a whole database with confidential personal information, even to a County PC or laptop. Such data should stay in the secure Data Center. The databases of public records, especially those in the County Clerk's Office, present special problems since these are required to be public. As the County has done in the past, it will continue to encourage and assist the County Clerk in redacting Social Security numbers from the images of those public records.

12. Contact Information

Submit all inquiries and requests for future enhancements to the owner at:

Marguerite Beirne, CIO
Reference: WC-P16-001
Westchester County Department of Information Technology
148 Martine Avenue, Room 313
White Plains, NY 10601
Phone: (914) 995-8161
Email: mcb1@westchestergov.com

13. Revision History

This policy shall be reviewed at least every year to ensure relevancy.

Date	Description of Change	Reviewer
01/01/2016	Original policy release	Scott Fernqvist
01/12/2023	Various updates and reformatting	Scott Fernqvist