



Personally Identifiable Information Policy

Policy Statement

It is the policy of the Town of Fenwick Island to protect personally identifiable information (PII) of employees and volunteers. The electronic restrictions and safeguards outlined in this policy provide guidance for employees and volunteers that have access to PII retained by the Town of Fenwick Island to ensure compliance with State and Federal regulations.

Definitions

Personally Identifiable Information (PII) is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered PII is available in public sources such as telephone books, public websites, etc. This type of information is considered to be public PII and includes:

1. First and last name
2. Address
3. Work telephone number
4. Work email address
5. Home telephone number
6. General educational credentials
7. Photos and videos

In contrast, protected PII is defined as any one or more of types of information including, but not limited to:

1. Social Security Number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Biometrics
8. Date and place of birth
9. Mother's maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Photos and videos including any of the above

Procedures

This section provides guidelines on how to maintain and discard PII. If current procedures fall outside this policy, or questions arise, please contact the Town Manager to suggest more efficient procedures for protecting PII. All electronic files that contained protected PII will reside within a protected information system location. All physical files that contain protected PII will reside within a locked file cabinet or room when not being actively viewed or modified. Protected PII is not to be downloaded to personal or Town of Fenwick Island owned employee or volunteer workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets, or removable media). PII will also not be sent through any form of insecure electronic communication (e.g., email or instant messaging systems). Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII, the physical or electronic file should be shredded or securely deleted.

Incident Reporting

The Town Manager must be informed of a real or suspected disclosure of protected PII data within 24 hours after discovery (e.g., misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII).

Audits

Periodic audits of Town of Fenwick Island owned equipment and physical locations may be performed to ensure that protected PII is stored in approved information systems or locations. The purpose of the audit is to ensure compliance with this policy and to provide information necessary to continuously improve practices.

Enforcement

An employee or volunteer found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation.

Records Disposal

Records containing personal data are to be disposed of so as to prevent inadvertent compromise of data. Paper records are disposed of by shredding or other method approved of by the National Institute of Standards and Technology. The disposal method will render all personal data unrecognizable and beyond reconstruction.