



Identity Protection

Purpose

The purpose of this policy is to protect the confidentiality, integrity, and security of Social Security numbers (SSNs) and other personally identifiable information collected or maintained by the Nippersink Public Library District ("Library"), in accordance with the Illinois Identity Protection Act (5 ILCS 179/1 et seq.).

This policy ensures that SSNs are collected and used only when legally required or essential to the Library's operations, and that they are safeguarded from unauthorized disclosure or misuse.

Policy Overview

The Library recognizes that improper collection, use, or disclosure of SSNs may facilitate identity theft and violate state law. The Library therefore:

1. Limits the collection and use of SSNs to those circumstances authorized by law or necessary for Library administration.
2. Implements administrative, technical, and physical safeguards to protect SSNs from unauthorized access, disclosure, alteration, or destruction.
3. Provides notice to individuals whenever SSNs are requested, stating the specific purpose for collection and how the number will be used.

Social Security Number Protection

The Library shall **not**:

- Publicly post or display an individual's SSN.
- Print an SSN on any card required to access Library services.
- Require transmission of an SSN over the Internet unless the connection is secure or the number is encrypted.
- Print an SSN on any materials mailed to an individual unless required by state or federal law, and never in a way that makes it visible without opening the envelope.
- Require an individual to use their SSN to access a website.
- Use an SSN for any purpose other than the one for which it was collected.

Authorized Collection and Use

The Library may collect, use, or disclose SSNs only when:

1. Required by state or federal law, rule, or regulation; or
2. Necessary to carry out the Library's legal duties and documented administrative purposes.

All such collections must:

- Document the specific need and purpose before collection; and
- Limit use strictly to the stated purpose.



Permitted disclosures include:

- To authorized Library employees, agents, contractors, or other governmental entities when necessary to perform official duties, provided that any contractor first supplies its own compliant identity-protection policy.
- Pursuant to court order, warrant, or subpoena.
- For legitimate internal verification, administrative, or law-enforcement purposes, including prevention of fraud or collection of lawful debts.

Redaction and Public Access

When responding to public-records requests under the Illinois Freedom of Information Act (5 ILCS 140/), the Library shall redact all but the last five digits of any SSN contained in a public document before release.

Records containing SSNs must be created and stored in a format that allows easy redaction if disclosure is required.

Employee Access and Training

Access to SSNs is restricted to employees whose job duties specifically require handling such information.

- Employees with authorized access shall receive training on safeguarding SSNs, secure handling procedures, and breach-response requirements.
- SSNs shall not be stored on portable drives or unencrypted devices.
- Digital systems containing SSNs must be protected through password-restricted accounts and secure, encrypted storage.

Breach Response and Compliance

If a potential or actual breach of SSN information occurs, the Library Director shall immediately take steps to mitigate harm, notify affected individuals as required by law, and report the incident to the Board of Trustees.

The Director shall review this policy periodically to ensure continued compliance with the Illinois Identity Protection Act and related state and federal regulations.