

## Operational Services

### Identity Protection <sup>1</sup>

The collection, storage, use, and disclosure of social security numbers by the School District shall be consistent with State and federal laws. The goals for managing the District's collection, storage, use, and disclosure of social security numbers are to: <sup>2</sup>

1. Limit all activities involving social security numbers to those circumstances that are authorized by State or federal law.
2. Protect each social security number collected or maintained by the District from unauthorized disclosure.

The Superintendent is responsible for ensuring that the District complies with the Identity Protection Act, 5 ILCS 179/. Compliance measures shall include each of the following: <sup>3</sup>

1. All employees having access to social security numbers in the course of performing their duties shall be trained to protect the confidentiality of social security numbers. Training should include instructions on the proper handling of information containing social security numbers from the time of collection through the destruction of the information.
2. Only employees who are required to use or handle information or documents that contain social security numbers shall have access to such information or documents.
3. Social security numbers requested from an individual shall be provided in a manner that makes the social security number easily redacted if the record is required to be released as part of a public records request.
4. When collecting a social security number or upon request by an individual, a statement of the purpose(s) for which the District is collecting and using the social security number shall be provided. <sup>4</sup>
5. All employees must be advised of this policy's existence and a copy of the policy must be made available to each employee. The policy must also be made available to any member of the public, upon request.

No District employee shall collect, store, use, or disclose an individual's social security number unless specifically authorized by the Superintendent. <sup>5</sup>

---

<sup>1</sup> The Identity Protection Act, 5 ILCS 179/, requires that this subject matter be covered in policy and controls its content. The Act places greater limits on the use of SSNs than federal law. The Act defines *identity-protection policy* as "any policy created to protect social security numbers from unauthorized disclosure." Thus, the policy will be sufficient if it focuses exclusively on protecting the privacy and confidentiality of social security numbers. Each district must implement its identity-protection policy before 6/1/2011 (5 ILCS 179/35). *Social security number* is not capitalized in the Identity Protection Act (5 ILCS 179/5).

<sup>2</sup> The list of goals is optional; it may be deleted, augmented, or otherwise amended.

<sup>3</sup> Items 1-4 in this numbered list must be covered in board policy (5 ILCS 179/35(a). Item #5 is not required to be in the policy but districts are required to do it (5 ILCS 179/35(b)). These compliance measures are covered in administrative procedure 4:15-AP, *Protecting the Privacy of Social Security Numbers*.

<sup>4</sup> See 4:15-E2, *Exhibit - Statement of Purpose for Collection of Social Security Numbers*.

<sup>5</sup> This sentence is optional. Its intent is to inform employees of the need to have proper authority before collecting, storing, using, or disclosing SSNs. A board may attach a sanction to the paragraph by adding the following option: "An employee who has substantially breached the confidentiality of social security numbers may be subject to disciplinary action or sanctions up to and including dismissal in accordance with District policy and procedures."

LEGAL REF.: 5 ILCS 179/, Identity Protection Act.

CROSS REF: 2:250 (Access to District Public Records), 5:150 (Personnel Records), 7:340 (Student Records)

**General Personnel**

**Administrative Procedure - Protecting the Privacy of Social Security Numbers**

Actor	Action
<p>Superintendent and business manager, and their designees</p>	<p>Identify the approved purposes for collecting SSNs, including:</p> <ol style="list-style-type: none"> <li>1. Employment matters, e.g., income reporting to IRS and the IL Dept. of Revenue, tax withholding, FICA, and Medicare.</li> <li>2. Verifying enrollment in various benefit programs, e.g., medical benefits, health insurance claims, and veterans' programs.</li> <li>3. Filing insurance claims.</li> <li>4. Internal verification or administrative purposes.</li> <li>5. Other uses authorized and/or required by State law including, without limitation, in the following circumstances (5ILCS 179/10(c):                         <ol style="list-style-type: none"> <li>a. Disclosing SSNs to another governmental entity if the disclosure is necessary for the entity to perform its duties and responsibilities;</li> <li>b. Disclosing a SSN pursuant to a court order, warrant, or subpoena; and</li> <li>c. Collecting or using SSNs to investigate or prevent fraud, to conduct background checks, to collect a debt, or to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act.</li> </ol> </li> </ol> <p>Identify a method for documenting the need and purpose for the SSN before its collection. 5 ILCS 179/10(b).</p> <p>Inform all employees of the District's efforts to protect the privacy of SSNs. See Exhibit 4:15-E1, <i>Letter to Employees Regarding Protecting the Privacy of Social Security Numbers</i>.</p> <p>While State law does not specifically require this step, the law contains mandates applicable to all employees that they need to know. Moreover, this letter provides an opportunity to increase awareness of the confidential nature of SSNs.</p> <p>Maintain a written list of each staff position that allows or requires access to SSNs.</p> <p>The existence of a written list, even though not required, is important for recordkeeping and accountability purposes.</p> <p>Require that employees who have access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. 5 ILCS 179/35(a)(2).</p> <p>Direct that only employees who are required to use or handle information or documents that contain SSNs have access to such information or documents. 5 ILCS 179/35(a)(3).</p>

<b>Actor</b>	<b>Action</b>
	<p>Require that SSNs requested from an individual be provided in a manner that makes the SSN easily redacted if the record is otherwise required to be released as part of a public records request. 5 ILCS 179/35(a)(4).</p> <p>Require that, when collecting a SSN or upon request a <i>statement of the purpose(s)</i> for which the District is collecting and using the SSN be provided. 5 ILCS 179/35(a)(5). See Exhibit 4:15-E2, <i>Letter to Employees Regarding Protecting the Privacy of Social Security Numbers</i>.</p> <p>Enforce the requirements in Board policy 4:15, <i>Identity Protection</i>, and this procedure.</p>
Records Custodian and Head of Information Technology (IT)	<p>Develop guidelines for handling social security numbers in electronic systems. These guidelines should address:</p> <ol style="list-style-type: none"> <li>1. The display of SSNs on computer terminals, screens, and reports;</li> <li>2. The security protocol for storing SSNs on a device or system protected by a password or other security system and for accessing SSNs that are included in part of an electronic database;</li> <li>3. The security protocol for deleting SSNs that are stored in electronic documents or databases; and</li> <li>4. Alternate mechanisms for integrating data other than the use of SSNs.</li> </ol>
Staff Development Head	<p>Design and execute a training program on protecting the confidentiality of SSNs for employees who have access to SSNs in the course of performing their duties.</p> <p>The training should include instructions on the proper handling of information that contains SSNs from the time of collection through the destruction of the information. 5 ILCS 179/35(a)(2).</p>
Assistant Superintendents, Directors, Building Principals, and/or Department Heads	<p>Require each staff member whose position allows or requires access to SSNs to attend training on protecting the confidentiality of SSNs.</p> <p>Instruct staff members whose position allows or requires access to SSNs to:</p> <ol style="list-style-type: none"> <li>1. Treat SSNs as confidential information.</li> <li>2. Never publically post or display SSNs or require any individual to verbally disclose his or her SSN.</li> <li>3. Dispose of documents containing SSNs in a secure fashion, such as, by shredding paper documents and by deleting electronic documents as instructed by the IT Department.</li> <li>4. Use SSNs as needed during the execution of their job duties and in accordance with the training and instructions that they received.</li> </ol>

Actor	Action
	Instruct staff members whose position does <u>not</u> require access to SSNs to notify a supervisor and/or the IT Department whenever a SSN is found in a document or other material, whether in paper or electronic form.
Freedom of Information Officer	Redact every SSN before allowing public inspection or copying of records responsive to a FOIA request. 5 ILCS 179/15.
Employees	<p>Do not collect, use, or disclose another individual's SSN unless directed to do so by an administrator.</p> <p><b>If the employee is in a position that requires access to SSNs:</b> Treat SSNs as confidential information and follow the instructions learned during training.</p> <p><b>If the employee is <u>not</u> in a position that requires access to SSNs:</b> Notify his or her supervisor and/or the IT Department whenever the employee comes across a document or other material, whether in paper or electronic form, that contains a SSN.</p>

**Operational Services**

**Exhibit - Letter to Employees Regarding Protecting the Privacy of Social Security Numbers**

*On District Letterhead*

Date

Re: Protecting the Privacy of Social Security Numbers (SSNs)

The Illinois Identity Protection Act, 5 ILCS 179/, contains requirements applicable to school districts and their employees. This letter’s purpose is to help you understand the protections and requirements of this law.

In implementing this law and the Board’s policy, I am seeking to:

1. Increase the awareness of the confidential nature of the SSN and the risk of identity theft related to unauthorized disclosure;
2. Have every employee understand that he or she is prohibited from collecting, displaying, or using another individual’s SSN unless authorized by a member of the District administrative staff; and
3. Ensure the use of consistent protocol regarding SSNs throughout the District.

I have copied below sections of the Identity Protection Act that must be followed by every school employee. I have also attached the School Board’s policy 4:15, *Identity Protection*. Please carefully read these documents. You will be contacted if you are scheduled to receive training on the protocol for collecting, using, maintaining, and disclosing SSNs.

An employee who has substantially breached the confidentiality of social security numbers may be subject to disciplinary action or sanctions up to and including dismissal, in accordance with District policy and procedures.

Sincerely,

Superintendent

\*\*\*\*\*

**Attachment #1: Relevant Sections from the Identity Protection Act, 5 ILCS 179/**

**Section 10. Prohibited Activities.**

- (a) Beginning July 1, 2010, no person or State or local government agency may do any of the following:
  - (1) Publicly post or publicly display in any manner an individual's social security number.
  - (2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity.
  - (3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.
  - (4) Print an individual's social security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail,

including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

- (b) Except as otherwise provided in this Act, beginning July 1, 2010, no person or State or local government agency may do any of the following:
  - (1) Collect, use, or disclose a social security number from an individual, unless (i) required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the social security number is documented before collection of the social security number; and (iii) the social security number collected is relevant to the documented need and purpose.
  - (2) Require an individual to use his or her social security number to access an Internet website.
  - (3) Use the social security number for any purpose other than the purpose for which it was collected.
- (c) The prohibitions in subsection (b) do not apply in the following circumstances:
  - (1) The disclosure of social security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's social security number will be achieved.
  - (2) The disclosure of social security numbers pursuant to a court order, warrant, or subpoena.
  - (3) The collection, use, or disclosure of social security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.
  - (4) The collection, use, or disclosure of social security numbers for internal verification or administrative purposes.
  - (5) The disclosure of social security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.
  - (6) The collection or use of social security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.
- (d) If any State or local government agency has adopted standards for the collection, use, or disclosure of social security numbers that are stricter than the standards under this Act with

respect to the protection of those social security numbers, then, in the event of any conflict with the provisions of this Act, the stricter standards adopted by the State or local government agency shall control.

**Section 15. Public inspection and copying of documents.**

Notwithstanding any other provision of this Act to the contrary, a person or State or local government agency must comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's social security number. A person or State or local government agency must redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.

**Section 20. Applicability.**

- (a) This Act does not apply to the collection, use, or disclosure of a social security number as required by State or federal law, rule, or regulation.
- (b) This Act does not apply to documents that are recorded with a county recorder or required to be open to the public under any State or federal law, rule, or regulation, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois. Notwithstanding this Section, county recorders must comply with Section 35 of this Act.

**Section 25. Compliance with federal law.**

If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, any State or local government agency that complies with the federal law shall be deemed to be in compliance with this Act.

**Section 30. Embedded social security numbers.**

Beginning December 31, 2009, no person or State or local government agency may encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology, or other technology, in place of removing the social security number as required by this Act.

**Section 45. Violation.**

Any person who intentionally violates the prohibitions in Section 10 of this Act is guilty of a Class B misdemeanor.

## Operational Services

### Exhibit - Statement of Purpose for Collecting Social Security Numbers <sup>1</sup>

This Statement of Purpose is being given to you because you have been asked by the School District to provide your social security number (SSN) or because you requested a copy of this Statement.

You are being asked for your SSN for one or more of the following reasons:

- Employment matters, e.g., income reporting to IRS and the IL Department of Revenue, tax withholding, FICA, or Medicare.
- Verifying enrollment in various benefit programs, e.g., medical or disability insurance and veterans' programs.
- Filing insurance claims.
- Internal verification or administrative purposes.
- Other: \_\_\_\_\_

In addition, State law authorizes and/or requires the District to use or disclose your SSN in specified circumstances including, without limitation, in the following circumstances:

1. Disclosing SSNs to another governmental entity if the disclosure is necessary for the entity to perform its duties and responsibilities;
2. Disclosing a SSN pursuant to a court order, warrant, or subpoena; and
3. Collecting or using SSNs to investigate or prevent fraud, to conduct background checks, to collect a debt, or to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act.

If you have questions or concerns, please contact *[insert contact information]*.

---

<sup>1</sup> The Identity Protection Act requires school districts, when collecting a social security number or upon request by an individual, to provide a statement of the purpose(s) for which the district is collecting and using the social security number (5 ILCS 179/35(a)(5)). State law does not require districts to retain evidence that the individual received the statement of purpose.

## **Operational Services**

### **Exhibit - Statement for Employee Manual or District Website Describing the District's Purpose for Collecting Social Security Numbers <sup>1</sup>**

The School District treats social security numbers (SSNs) confidentially. It uses SSNs for one or more of the following reasons:

1. Employment matters, e.g., income reporting to IRS and the IL Department of Revenue, tax withholding, FICA, or Medicare.
2. Verifying enrollment in various benefit programs, e.g., medical or disability insurance and veterans' programs.
3. Filing insurance claims.
4. Internal verification or administrative purposes.

In addition, State law authorizes and/or requires the District to use or disclose SSNs in specified circumstances including, without limitation, in the following circumstances:

4. Disclosing SSNs to another governmental entity if the disclosure is necessary for the entity to perform its duties and responsibilities;
5. Disclosing a SSN pursuant to a court order, warrant, or subpoena; and
6. Collecting or using SSNs to investigate or prevent fraud, to conduct background checks, to collect a debt, or to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act.

If you have questions or concerns, please contact *[insert contact information]*.

Reviewed March 2011

Adopted April 2011

---

---

<sup>1</sup> The Identity Protection Act requires school districts, when collecting a SSN or upon request by an individual, to provide a statement of the purpose(s) for which the district is collecting and using the SSN (5 ILCS 179/35(a)(5)). State law does not require districts to retain evidence that the individual received the statement of purpose.

