Operational Services

Identity Protection [1]

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:[2]

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:[3]

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.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

1 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." *Social security number* is not capitalized in the Identity Protection Act. 5 ILCS 179/5.

Another State law, the Personal Information Protection Act, 815 ILCS 530/, amended by P.A. 99-503~~97-483~~, contains mandates for *government agencies* and *local governments* and may apply to school districts. ~~Attorneys disagree whether this Act applies to school districts.~~ This Act contains requirements for: (1) notifying an owner of a security breach, and (2) disposing of material containing *personal information* (defined as the owner's name combined with SSN, driver's license number or State identification card number, and financial account information, including without limitation, credit or debit card numbers).

Much of a district's collection, storage, use, and disclosure of social security numbers applies to employee records only. But limited exceptions may exist where a school district may need to ask students or their parents/guardians to provide social security numbers, and any collection and retention of student's social security numbers must also be in accordance with this policy.

Consult the board attorney before adoption of this policy. Districts may choose to provide or implement more protections than the statutory requirements outlined in this sample policy. Technology and best practices are constantly changing. While the laws that apply to this policy govern current management of sensitive information, best practices may outpace the law's ability to keep up.

See also f/n19 to sample policy 2:250, *Access to District Public Records*, detailing the preservation requirements of the Local Records Act~~,~~ (50 ILCS 205/3). the Family Educational Rights and Privacy Act~~,~~ (20 U.S.C. §1232g), and the Ill. School Student Records Act~~,~~ (105 ILCS 10/), and litigation holds or ~~a~~ document preservation requirements pursuant to Federal Rules of Civil Procedure~~,~~ (Rules 16 and 26).

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

3 The Identity Protection Act, 5 ILCS 179/35(a) requires ~~I~~items #1-4 ~~in this numbered list must~~ to be covered in a ~~board~~ policy. ~~5 ILCS 179/35(a).~~

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.**4**

5. Notification to an individual as required by 815 ILCS 530/12 whenever his or her personal information was acquired by an unauthorized person; *personal information* means either:

   a. ~~(a)is a~~An individual's first name or first initial and last name in combination with any one or more of~~with~~ his or her (i) social security number, (ii) driver's license number or State identification card number, ~~or~~ (iii) financial account information (with any required security codes or passwords), (iv) medical information, (v) health insurance information, and/or (vi) unique biometric data or other unique physical or digital representation of biometric data, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired through the breach of security; or

   ~~a.~~b. ~~(b) a~~An individual's username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the username or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.**5**

6. Disposal of materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable; *personal information* has the meaning stated in #5, above.

7. Notification, within 45 days of the discovery of a security breach, to the Illinois Attorney General:

   a. If the District suffers a breach of more than 250 Illinois residents; or

   ~~a.~~b. When the District provides notice as required in #5, above.**6**

~~5.~~8. 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.**7**

No District employee shall collect, store, use, or disclose an individual's social security number unless specifically authorized by the Superintendent.**8** This policy shall not be interpreted as a guarantee of the confidentiality of social security numbers and/or other personal information. The District will use best efforts to comply with this policy, but this policy should not be construed to convey any rights to protection of information not otherwise afforded by law.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

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

5 Items #5 and ~~&~~ #6 are not required to be in policy. They are mandates contained in the Personal Information Protection Act; see the second paragraph of f/n #1. They are included in the sample policy because: (1) they are consistent with public policy, and (2) if the Act applies to school districts, so will its section allowing the Attorney General to fine any person up to $100 for each violation of the disposal requirements for materials containing personal information. 815 ILCS 530/40, amended by P.A. 99-503.

6 815 ILCS 530/12, (e), amended by P.A. 99-503. Notification sooner is preferred, if it can be accomplished.

7 Item #~~8~~7 is not required to be in ~~the~~ policy but districts are required to perform the described action (5 ILCS 179/35(b)). These compliance measures are covered in administrative procedure 4:15-AP, *Protecting the Privacy of Social Security Numbers.*

8 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 SSNs 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.
50 ILCS 205/3, Local Records Act.
105 ILCS 10/, Illinois School Student Records Act.
815 ILCS 530/, Personal Information Protection Act.

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