DRAFT UPDATE

Operational Services

Identity Protection

Commented [APowell1]:
The Identity Protection Act, 5 ILCS 179/ requires policy about identity protection and controls the policy's content. The Act defines *identity-protection policy* as "any policy created to protect social security numbers from unauthorized disclosure." This law contrasts with the Personal Information Protection Act discussed below, which may apply to school districts.

Issue 94, March 2017

This policy addresses the District's handling of personal information, which includes social security numbers, driver's license numbers, State identification card numbers, and financial account information.

Social Security Numbers

The collection, storage, use, and disclosure of social security numbers by the School District shall be consistent with State and federal laws. The Superintendent is responsible for ensuring that the District complies with the Identity Protection Act, 5 ILCS 179/et seq. Compliance measures shall include the following:

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 shall include instructions on the proper handling of information containing social security numbers from the time of collection through the destruction of the information. Training shall also include notification that no District employee may collect, store, use, or disclose an individual's social security number unless specifically authorized by the Superintendent.
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. If a social security number is requested from an individual, it shall be maintained in any document in a manner that is easily redactable 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.
5. Notification to an individual as required by §15 ILCS 530/12 whenever his or her personal information was acquired by an unauthorized person. *personal information* means either:
   a. An individual's first name or first initial and last name in combination with any one or more of his or her (i) social security number, (ii) driver's license number or State identification card number, (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. 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. 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.

Commented [APowell2]:
Updated in response to the Personal Information Protection Act, 815 ILCS 530/, amended by P.A. 99-503, which contains mandates for *government agencies* and *local governments*, and may apply to school districts.

Consult the Board attorney before adoption of this policy. Districts may choose to provide or implement more protections than the statutory requirements outlined here. Technology and best practices are constantly changing.

Issue 94, March 2017

DRAFT UPDATE

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.

~~5.~~ 8. All employees must be advised of this policy's existence and the existence of any amendment thereto and a copy of the policy and any amendment thereto must be made available to each employee. The policy and any amendment thereto must also be made available to any member of the public, upon request.

Commented [APowell3]:
815 ILCS 530-12.(c), amended by P.A. 99-503.
Notification sooner is preferred, if it can be accomplished.

Issue 94, March 2017

Breaches of Personal Information

If a breach occurs in which an unauthorized person obtains an individual's name or first initial and last name in combination with any personal information for that individual, the Superintendent shall determine what, if any, notification shall be given to the individual whose information was obtained. In making that determination, the Superintendent shall consider and comply with any relevant laws and shall consider, even where no legal mandates for notification exist, whether notification is in the best interest of the District.

Disposal of Personal Information

The Superintendent shall dispose of materials containing personal information in a manner that complies with any relevant laws and considers the best interest of the District.

Limitations

This policy shall not be interpreted as a guarantee of the confidentiality of personal information, including social security numbers. 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.

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)

ADOPTED: ~~July 18, 2013~~