DRAFT UPDATE

Operational Services

Identity Protection

The collection, storage, use, and disclosure of social security numbers by the Cooperative shall be consistent with State and federal laws. The goals for managing the Cooperative's collection, storage, use, and disclosure of social security numbers are to:

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 Cooperative from unauthorized disclosure.

The Executive Director or designee is responsible for ensuring that the Cooperative complies with the Identity Protection Act, 5 ILCS 179/. Compliance measures shall include each of 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 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 Cooperative is collecting and using the social security number shall be provided. The stated reason for collection of the social security number must be relevant to the documented purpose.
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. ~~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~~
   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.~~
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.~~

Delete #s 5, 6, 7.

Commented [AP1]: In response to some Ill. Council of School Attorneys' opinions regarding the questionable application of the Personal Information Protection Act (PIPA, 815 ILCS 530/) to school districts, PIPA requirements have been deleted.

Consult the Board attorney before adoption of this policy. Districts may choose to provide or implement more protections than the statutory requirements outlined here.

OPTION: For Boards that have consulted with their attorney and want to include PIPA mandates in this Policy, "815 ILCS 530/, Personal Information Protection Act" will be added to the Legal References, and the following will be added as another paragraph immediately after this numbered list:

The Superintendent is also responsible for ensuring the District complies with the Personal Information Protection Act, 815 ILCS 530/. Compliance measures shall include each of the following:
1. Written or electronic 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. 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
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.
2. 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 #1, above.
3. Notification, no later than 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
   b. When the District provides notice as required in #1, above.

Issue 96, October 2017

Add, "In the event of a breach in the security of an employee's social security number or other similar private information, the Executive Director will inform the Board and consult with legal counsel to determine what action, if any, should be taken by the Cooperative."

DRAFT UPDATE

~~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~~

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

~~8.~~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.

6. If this policy is amended, employees will be advised of the existence of the amended policy and a copy of the amended policy will be made available to each employee.

No Cooperative employee shall collect, store, use, or disclose an individual's social security number unless specifically authorized by the Executive Director.

Commented [AP2]: Items #5 and #6 are not required to be in policy, but districts are required to perform the described actions. 5 ILCS 179/35(b). These compliance measures are covered in 4:15-AP, *Protecting the Privacy of Social Security Numbers*.

Issue 96, October 2017

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 Cooperative Public Records), 5:150 (Personnel Records), 7:340 (Student Records)

ADOPTED: ~~May 31, 2017~~