DRAFT UPDATE

Operational Services

Identity Protection

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:

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:

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.
5. Notification to an individual whenever his or her personal information was acquired by an unauthorized person; *personal information* is an individual's name in combination with his or her social security number, driver's license number or State identification card number, or financial account information.
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. ~~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. 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.

Comment [AKL1]:
UPDATE 1: Suggested items #5 & #6 are not required to be in policy. They are mandates contained in the Personal Information Protection Act.
Attorneys disagree whether the Act applies to school districts; however,
the mandates 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).

Issue 81, March 2013

Comment [AKL2]:
UPDATE 2: A disclaimer is offered; however, the usefulness of the disclaimer is untested and unproven.

Issue 81, March 2013

DRAFT UPDATE

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)

ADOPTED: ~~December 13, 2011~~