4:15 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. The stated reason for collection of the social security number must be relevant to the documented purpose.
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.

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 and, if applicable, the owner of the information, as required by 815 ILCS 530/10 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. Notification to the Ill. Attorney General as required by 815 ILCS 530/10, if a single breach of the security system requires the District to notify more than 500 Illinois residents.
3. Cooperation with the owner of the information in matters relating to the breach, if applicable, as required by 815 ILCS 530/10.
4. 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.

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

Treatment of Personally Identifiable Information Under Grant Awards

The Superintendent ensures that the District takes reasonable measures to safeguard: (1) *protected personally identifiable information*, (2) other information that a federal awarding agency, pass-through agency or State awarding agency designates as

sensitive, such as *personally identifiable information* (PII) and (3) information that the District considers to be sensitive consistent with applicable laws regarding privacy and confidentiality (collectively, *sensitive information)*, when administering federal grant awards and State grant awards governed by the Grant Accountability and Transparency Act (30 ILCS 708/).

The Superintendent shall establish procedures for the identification, handling, storage, access, disposal and overall confidentiality of sensitive information. The Superintendent shall ensure that employees and contractors responsible for the administration of a federal or State award for the District receive regular training in the safeguarding of sensitive information. Employees mishandling sensitive information are subject to discipline, up to and including dismissal.

LEGAL REF.:

2 C.F.R. §200.303(e).

5 ILCS 179/, Identity Protection Act.

30 ILCS 708/, Grant Accountability and Transparency 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: January 15, 2020