Document Status: Draft Update

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.
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.
7. 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.[PRESSPlus1]
8. ~~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.~~
9. 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.

Treatment of Personally Identifiable Information Under Grant Awards[PRESSPlus2]

The Superintendent ensures that the District takes reasonable measures to safeguard: (1) *protected personally identifiable information*,[PRESSPlus3] (2) other information that a federal awarding agency, pass-through agency or State awarding agency designates as sensitive, such as *personally identifiable information* (PII)[PRESSPlus4] 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.[PRESSPlus5] 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: September 28, 2017

PRESSPlus Comments

PRESSPlus 1. Personal Information Protection Act, amended by P.A. 101-343, eff. 1-1-20. **Issue 102, October 2019**

PRESSPlus 2. Added in response to the Ill. State Board of Education's *Checklist for Protection of Personally Identifiable Information Review* (ISBE Checklist) and the Grant Accountability and Transparency Act (GATA) (30 ILCS 708/).

See the ISBE Checklist at www.isbe.net/Pages/Audit-and-Monitoring-Review-Requirements-and-Tools.aspx.

While the federal regulations on procurement standards in 2 C.F.R. Part 200 do not specifically require a written policy on the treatment of *personally identifiable information* (PII) under grant-funded programs, the the ISBE Checklist requires an approved policy or policies related to the identification, handling, storage, access, disposal, and overall protection of PII as evidence of legal compliance with GATA and federal regulations. The ISBE Checklist is specific to PII handled by districts in connection with their administration of grants. The uniform federal rules on procurement standards in 2 C.F.R. Part 200 apply to eligible State grants through GATA. This policy and administrative procedure 4:15-AP2, *Personally Identifiable Information Under Grant Awards*, (available by logging into PRESS Online at iasb.com) are designed to help districts meet the standard set forth in 2 C.F.R. 200.303(e) and the documentation items on the ISBE Checklist.

The Ill. State Board of Education (ISBE) considers the Personal Information Protection Act (PIPA) (815 ILCS 530/, amended by P.A. 101-343, eff. 1-1-20) to apply to the handling of personally identifiable information under grant awards. Consult the board attorney for advice on the broader applicability of PIPA's mandates to your district.

Issue 102, October 2019

PRESSPlus 3. *Protected personally identifiable information* (Protected PII) means an individual's first name or first initial and last name in combination with any one or more types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal records, medical records, financial records, or educational transcripts. 2 C.F.R. §200.82. **Issue 102, October 2019**

PRESSPlus 4. Protected PII is a subset of PII. PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books and public websites, and it is considered to be Public PII. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. 2 C.F.R. §200.79.

In addition to 2 C.F.R. 200.303(e), depending upon the type of record being created or used in connection with a grant-funded program, multiple laws may govern the treatment of *personally identifiable information* (PII) under a grant, including the IPA (5 ILCS 179/), PIPA (815 ILCS 530/), Family Educational Rights and Privacy Act, (20 U.S.C. 1232g), Ill. School Student Records Act (105 ILCS 10/), Student Online Personal Protection Act, (105 ILCS 85/, amended by P.A. 101-516, eff. 7-1-21), Personnel Record Review Act (820 ILCS 40/), and Local Records Act (50 ILCS 205/3).

Issue 102, October 2019

PRESSPlus 5. The ISBE Checklist requires districts to maintain documentation of training of all employees/contractors on the handling of PII, including evidence of the date(s) of the training and attendance/completion of the training. Because many individuals in a district can be involved in day-to-day administration of activities supported by a federal or State grant, best practice is to regularly train all employees on the safeguarding of such sensitive information, e.g., upon hire and then annually or semi-annually. **Issue 102, October 2019**