Document Status: Draft Update

OPERATIONAL SERVICES

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.

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

Treatment of Personally Identifiable Information Under Grant Awards

The Superintendent ensures that the District takes reasonable cybersecurity and other measures to safeguard information including:PRESSPlus1 (1) *protected personally identifiable information*, (2) other types of information that a federal ~~awarding~~ agency, pass-through ~~agency~~entity, 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.

CROSS REF: 2:250 (Access to District Public Records), 5:150 (Personnel Records), 7:340 (Student Records), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

Adopted: August 15, 2024

PRESSPlus Comments

PRESSPlus 1. Updated in response to 2 C.F.R Part 200, amended by 89 Fed. Reg 30046, addressing the safeguarding of information under grant awards and updating the definitions for *personally identifiable information* and *protected personally identifiable information*.

*Personally Identifiable Information (*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 PII is available in public sources such as telephone books and websites. This was previously defined as *public personally identifiable information* (Public PII), but 2024 revisions to 2 C.F.R. Part 200 have deleted Public PII as a definition. The definition of PII is not attached to any single category of information or technology. Instead, 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 could be used to identify an individual when combined with other available information. 2 C.F.R. §200.1.

Protected personally identifiable information (Protected PII) means PII, except for certain types of PII that must be disclosed by law. 2024 revisions to 2 C.F.R. Part 200 eliminated examples of Protected PII and instead only list examples of PII within the definition of Protected PII at 2 C.F.R. §200.1, which may indicate broadening of the definition of Protected PII. See 89 Fed. Reg. 79732. Before the 2024 revisions, examples of Protected PII contained in the regulation included, but were 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, and educational transcripts. 2 C.F.R. §200.1. Consult the board attorney for guidance in this area. See sample administrative procedure 4:15-AP2, *Treatment of Personally Identifiable Information Under Grant Awards*, available at PRESS Online by logging in at www.iasb.com. Protected PII is similar to,

but broader than, the definition of *personal information* under PIPA. **Issue 118, April 2025**