## Identity Protection

The collection, storage, use, and disclosure of social security numbers by the District 99 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.

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

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

Adopted: 1/28/13
Revised: 11/18/13; 7/17/17; 3/19/18; 3/16/20; 10/20/25