

## Operational Services

### Personally Identifiable Information Protection

Personally identifiable information (PII), is information which, when disclosed, could result in harm to the individual whose privacy has been breached. Such information includes biometric information, medical information, personally identifiable financial information and unique identifiers such as passport or Social Security numbers. The collection, storage, use, and disclosure of personally identifiable information 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 personally identifiable information is to:

1. Limit all activities involving personally identifiable information, birth dates and other personally identifiable information to those circumstances as contemplated by State or federal law including but not limited to;
  - i. Employee benefit processing, including membership in the Illinois Municipal Retirement System, Teacher's Retirement System, District sponsored health, dental and life insurance, or other benefits offered to employees by the School Board;
  - ii. Compliance with the reporting requirements for the Internal Revenue Service, Social Security Administration, Illinois Department of Employment Security, and such other official reporting responsibilities imposed by law;
  - iii. Processing E-Verify forms;
  - iv. For purpose of determining eligibility under State or federal school lunch and breakfast programs;
  - v. Submitting bills for medically related services outlined in students' IEPs to Medicaid when authorized by parents/guardians;
  - vi. For such purposes as may be directed by the employee, such as direct deposit of wages or salary, payroll deductions, etc; and
  - vii. Pursuant to a court order, warrant, subpoena or collective bargaining agreement.
2. Protect personally identifiable information 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 179/1 et seq.* Compliance measures shall include each of the following:

1. Employees having access to personally identifiable information in the course of performing their duties may be required to take training on how to protect the confidentiality of personally identifiable information. Training should include instructions on the proper handling of information containing personally identifiable information 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 personally identifiable information shall have access to such information or documents.
3. Personally identifiable information requested from an individual shall be provided in a manner that makes the personally identifiable information easily redacted if the record is required to be released as part of a public records request.
4. When collecting a personally identifiable information or upon request by an individual, a statement of the purpose(s) for which the District is collecting and using the personally identifiable information shall be provided.  
  
Notification to an individual whenever his or her personal information was acquired by an unauthorized person.
5. Disposal of materials containing personally identifiable information, as personally identifiable information is defined in this policy, in a manner that renders the personal information unreadable, unusable, and undecipherable.
6. 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 personally identifiable information unless specifically authorized by the Superintendent or designee. This policy shall not be interpreted as a guarantee of the confidentiality of personally identifiable information 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 PII Under Grant Awards

The Superintendent ensures that the District takes reasonable measures to safeguard: (1) PII, (2) other information that a federal awarding agency, pass-through agency or State awarding agency designates as sensitive, 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.: Two C.F.R. §200.303(e); five ILCS 179/1 ET. seq., *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*.

<sup>2</sup> CROSS REF.: 2.250, 5.150, 7.340

Adopted: August 14, 2012

Revised: March 22, 2016  
February 11, 2020