Operational Services

Identity Protection [1]

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: [2]

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 footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[1] **Consult the board attorney before adoption of this policy**. Districts may choose to provide or implement more protections than the statutory requirements outlined in this sample policy. While the laws that apply to this policy govern current management of sensitive information, best practices may outpace the law's ability to keep up. See also f/n 19 to sample policy 2:250, *Access to District Public Records*, detailing the preservation requirements of the Local Records Act (50 ILCS 205/3), the Family Educational Rights and Privacy Act (20 U.S.C. §1232g), and the Ill. School Student Records Act (105 ILCS 10/), and litigation holds or document preservation requirements pursuant to Federal Rules of Civil Procedure (Rules 16 and 26).

The Identity Protection Act (IPA) (5 ILCS 179/) requires that this subject matter be covered in policy and controls its content. 5 ILCS 179/35. The Act places greater limits on the use of social security numbers (SSNs) than federal law. The IPA defines *identity-protection policy* as "any policy created to protect social security numbers from unauthorized disclosure." (*Social security number* is not capitalized in the IPA). 5 ILCS 179/5. Much of a district's collection, storage, use, and disclosure of SSNs applies to employee records only. But limited exceptions may exist where a school district may need to ask students or their parents/guardians to provide SSNs, and any collection and retention of students' SSNs must also be in accordance with this policy.

Another State law, the Personal Information Protection Act (PIPA) (815 ILCS 530/) requires *data collectors of personal information* to provide certain notice to Illinois residents, and in certain cases, the Ill. Attorney General, when the collector's system data is breached. 815 ILCS 530/10. Under PIPA, *data collector* is broadly defined to include government agencies and any entities that deal with nonpublic *personal information*. *Personal information* is defined as: (1) an individual's first name or first initial combined with an SSN, driver's license number or State identification card number, financial account information (including without limitation, credit or debit card numbers), medical or health insurance information or biometric data; or (2) a username or email address in combination with a password or security question and answer that would permit access to an online account. Id. at 530/5. Depending on whether the *data collector* owns or merely maintains or stores the information, additional notification requirements will also apply. Finally, PIPA requires *units of local governments* to dispose of personal information so that it may not be read or reconstructed. Id. at 530/40. It is unclear whether Section 530/40 applies to school districts because PIPA does not specifically identify school districts as *units of local governments* (Ill. Constitution Article VII, Sec. 1). However, the Ill. State Board of Education (ISBE) considers PIPA to apply to the handling of personally identifiable information under grant awards. See the ISBE *Checklist for Protection of Personally Identifiable Information Review*, referenced in f/n 9, below. **Consult the board attorney for advice on the applicability of PIPA's various mandates to your district**. See f/n 4, below for more information about options to include PIPA requirements in this sample policy.

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) recommends that K-12 districts have an *incident response plan* (IRP) that details what a district needs to do before, during, and after an actual or potential security incident. See www.cisa.gov/online-toolkit-partnering-safeguard-k-12-organizations-cybersecurity-threats. In the case of a data breach, it is critical for a district to have an IRP in place that is customized to local conditions and to practice the plan. Having an IRP may also be required for cyber liability insurance coverage. For resources and templates, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, www.ltcillinois.org/resources/k12-incident-response-plan-template-security-studio, https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings, and www.k12six.org/essentials-series.

[2] The list of goals is optional; it may be deleted, augmented, or otherwise amended.

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: [3] [4]

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]
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]

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[3] The IPA requires items #1-4 to be covered in a policy. 5 ILCS 179/35(a).

[4] For boards that want to include PIPA mandates in this Policy, insert the following option after the IPA items #1-4, or if the board includes items #5 and #6 (discussed in f/n 6, below), after items #1-6, and add "815 ILCS 530/, Personal Information Protection Act" to the Legal References:

> 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.

[5] See sample exhibit 4:15-E2, *Statement of Purpose for Collection of Social Security Numbers*.

[6] Items #5 and #6 are not required to be in policy but districts are required to perform the described action(s). 5 ILCS 179/35(b). These compliance measures are covered in sample administrative procedure 4:15-AP1, *Protecting the Privacy of Social Security Numbers*.

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. [7]

No District employee shall collect, store, use, or disclose an individual's social security number unless specifically authorized by the Superintendent.[8] 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 [9]

The Superintendent ensures that the District takes reasonable cybersecurity and other measures to safeguard information including: (1) *protected personally identifiable information*,[10] (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)[11] and (3) information that the District considers to be

---

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[7] Optional. See f/n 6 above.

[8] This sentence is optional. Its intent is to inform employees of the need to have proper authority before collecting, storing, using, or disclosing SSNs. A board may attach a sanction to the paragraph by adding the following option:

> 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.

[9] 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 Ill. State Board of Education's (ISBE's) *Checklist for Protection of Personally Identifiable Information Review* (ISBE Checklist), at www.isbe.net/Pages/Federal-and-State-Monitoring.aspx, 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 the Grant Accountability and Transparency Act (GATA) (30 ILCS 708/) and federal regulations. At the time of **PRESS** Issue 118's publication (Apr. 2025), ISBE had not updated this Checklist with the 2024 revisions to the definitions of PII and *protected personally identifiable information* (Protected PII) at 2 C.F.R. §200.1. 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 the Grant Accountability and Transparency Act (GATA) (30 ILCS 708/). This sample policy and accompanying sample administrative procedure 4:15-AP2, *Treatment of Personally Identifiable Information Under Grant Awards*, 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.

[10] Protected PII means PII (see definition at f/n 11), 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*. Protected PII is similar to, but broader than, the definition of *personal information* under PIPA.

[11] PII is a broader concept than Protected PII. Said another way, 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 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.

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.[12] 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.[13] 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)

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

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 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/), Personnel Record Review Act (820 ILCS 40/), and Local Records Act (50 ILCS 205/3).

[12] See sample administrative procedure 4:15-AP2, *Treatment of Personally Identifiable Information Under Grant Awards*.

[13] 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. See www.isbe.net/Pages/Federal-and-State-Monitoring.aspx. 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.