Operational Services

Administrative Procedure - Protecting the Privacy of Social Security Numbers

Much of the District's collection, storage, use, and disclosure of social security numbers apply to employee records only. But limited exceptions may exist where a school district may need to ask students or their parents/guardians to provide social security numbers. When student social security numbers are involved, consult the Board attorney about the intersection of the Identity Protection Act (5 ILCS 179/), the Family Educational Rights and Privacy Act (20 U.S.C. §1232g), and the Ill. School Student Records Act (105 ILCS 10/).

Actor	Action
Superintendent and business manager, and their designees	Identify the approved purposes for collecting SSNs, including: 1. Employment matters, e.g., income reporting to IRS and the IL Dept. of Revenue, tax withholding, FICA, and Medicare. 2. Verifying enrollment in various benefit programs, e.g., medical benefits, health insurance claims, and veterans' programs. 3. Filing insurance claims. 4. Internal verification or administrative purposes. 5. Other uses authorized and/or required by State law including, without limitation, in the following circumstances (5 ILCS 179/10(c)): a. Disclosing SSNs to another governmental entity if the disclosure is necessary for the entity to perform its duties and responsibilities; b. Disclosing SSNs pursuant to a court order, warrant, or subpoena; and c. Collecting or using SSNs to investigate or prevent fraud, to conduct background checks, to collect a debt, or to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act. Identify a method for documenting the need and purpose for the SSN before its collection. 5 ILCS 179/10(b)(1). Inform all employees of the District's efforts to protect the privacy of SSNs. See Exhibit 4:15-E1, *Letter to Employees Regarding Protecting the Privacy of Social Security Numbers*. While State law does not specifically require this step, the law contains mandates applicable to all employees that they need to know. Moreover, this letter provides an opportunity to increase awareness of the confidential nature of SSNs.

Actor	Action
	Maintain a written list of each staff position that allows or requires access to SSNs. The existence of a written list, even though not required, is important for recordkeeping and accountability purposes. Require that employees who have access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. 5 ILCS 179/35(a)(2). Direct that only employees who are required to use or handle information or documents that contain SSNs have access to such information or documents. 5 ILCS 179/35(a)(3). Require that SSNs requested from an individual be provided in a manner that makes the SSN easily redacted if the record is otherwise required to be released as part of a public records request. 5 ILCS 179/35(a)(4). Require that, when collecting SSNs or upon request, a *statement of the purpose(s)* for which the District is collecting and using the SSNs be provided. 5 ILCS 179/35(a)(5). See Exhibit 4:15-E2, *Statement of Purpose for Collecting Social Security Numbers*. Require that, when employees who are required to use or handle information or documents that contain SSNs learn of a breach, they: 1. Notify District administrators immediately, and 2. Ensure that notifications to the proper individuals occur, including the notifications listed within the Illinois Attorney General's guidance document on pages 7-11 at: www.illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf. Enforce the requirements in Board policy 4:15, *Identity Protection*, and this procedure.
Records Custodian and Head of Information Technology (IT)	Develop guidelines for handling social security numbers in electronic systems. These guidelines should address: 1. The display of SSNs on computer terminals, screens, and reports; 2. The security protocol for storing SSNs on a device or system protected by a password or other security system and for accessing SSNs that are included in part of an electronic database; 3. The security protocol for deleting SSNs that are stored in electronic documents or databases; and 4. Alternate mechanisms for integrating data other than the use of SSNs.

Staff Development Head	Design and execute a training program on protecting the confidentiality of SSNs for employees who have access to SSNs in the course of performing their duties. The training should include instructions on the proper handling of information that contains SSNs from the time of collection through the destruction of the information. 5 ILCS 179/35(a)(2).
Assistant Superintendents, Directors, Building Principals, and/or Department Heads	Require each staff member whose position allows or requires access to SSNs to attend training on protecting the confidentiality of SSNs. Instruct staff members whose positions allow or require access to SSNs to: 1. Treat SSNs as confidential information. 2. Never publically post or display SSNs or require any individual to verbally disclose his or her SSN. 3. Dispose of documents containing SSNs in a secure fashion, such as, by shredding paper documents and by deleting electronic documents as instructed by the IT Department. 4. Use SSNs as needed during the execution of their job duties and in accordance with the training and instructions that they received. Instruct staff members whose positions do <u>not</u> require access to SSNs to notify a supervisor and/or the IT Department whenever SSNs are found in a document or other material, whether in paper or electronic form.
Freedom of Information Officer	Redact every SSN before allowing public inspection or copying of records responsive to a FOIA request. 5 ILCS 179/15.
Employees	Do not collect, use, or disclose another individual's SSN unless directed to do so by an administrator. **If the employee is in a position that requires access to SSNs:** Treat SSNs as confidential information and follow the instructions learned during training. **If the employee is <u>not</u> in a position that requires access to SSNs:** Notify his or her supervisor and/or the IT Department whenever the employee comes across a document or other material, whether in paper or electronic form, that contain SSNs.