

PERSONNELGENERAL PERSONNEL - IDENTITY PROTECTIONThe Illinois Identity Protection Act

Due to increased incidents of fraud and identity theft, the Illinois Identity Protection Act (5 ILCS 179/1 *et seq.*) was adopted to help prevent the unauthorized collection, use and disclosure of employee social security numbers (the "Illinois Identity Protection Act" or the "Act"). Community Consolidated School District 93 adopts this policy pursuant to requirements of the Act.

Prohibited Activities Under the Act

- (a) Pursuant to the provisions of the Act, neither the School District nor any District employee may do any of the following:
- (1) Publicly post or publicly display in any manner an individual's social security number.
 - (2) Print an individual's social security number on any card required for the individual to access products or services provided by the District or employee.
 - (3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.
 - (4) Print an individual's social security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the social security number to be on the document to be mailed.

Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. However, a social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

- (b) Except as otherwise provided in the Illinois Identity Protection Act or this policy, neither the District, nor any District employee, may do any of the following:
- (1) Collect, use, or disclose a social security number from an individual, unless (i) required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the social security number is documented before collection of the social security number; and (iii) the social security number collected is relevant to the documented need and purpose.

PERSONNELGENERAL PERSONNEL - IDENTITY PROTECTION

- (2) Require an individual to use his or her social security number to access an Internet website.
 - (3) Use the social security number for any purpose other than the purpose for which it was collected.
- (c) The prohibitions in subsection (b) above do not apply in the following circumstances:
- (1) The disclosure of social security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's social security number will be achieved.
 - (2) The disclosure of social security numbers pursuant to a court order, warrant, or subpoena.
 - (3) The collection, use, or disclosure of social security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.
 - (4) The collection, use, or disclosure of social security numbers for internal verification or administrative purposes.
 - (5) The disclosure of social security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.
 - (6) The collection or use of social security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.
- (d) If the District adopts, or has adopted, standards for the collection, use, or disclosure of social security numbers that are stricter than the standards under the Illinois Identity Protection Act with respect to the protection of those social security numbers, then, in the event of any conflict with the provisions of the Act, the stricter standards adopted by the District shall control.

PERSONNEL

GENERAL PERSONNEL - IDENTITY PROTECTION

Persons With Access to Social Security Numbers

Only those District employees who are required to use or handle information or documents that contain social security numbers have access to such information or documents.

Collection of Social Security Numbers

Pursuant to the provisions of the Illinois Identity Protection Act, any social security number requested from an individual will be provided in a manner that makes the social security number easily redacted if required to be released as part of a public records request. When collecting a social security number or upon request by the individual, a statement of the purpose or purposes for which the District is collecting and using the social security number will be provided.

Public Inspection and Copying of Documents

Notwithstanding any other provision of the Act to the contrary, the District and all District employees must comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's social security number. The District and all District employees must redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.

Applicability

Neither the Illinois Identity Protection Act, nor this policy, will apply to the following:

- (a) The collection, use, or disclosure of a social security number as required by State or federal law, rule, or regulation.
- (b) Documents that are recorded with a county recorder or required to be open to the public under any State or federal law, rule, or regulation, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.

Compliance with Federal Law

If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, the District shall be deemed to be in compliance with the Illinois Identity Protection Act if the District complies with that federal law.

Embedded Social Security Numbers

Neither the District, nor any District employee, may encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology, or other technology, in place of removing the social security number as required by the Illinois Identity Protection Act.

PERSONNEL

GENERAL PERSONNEL - IDENTITY PROTECTION

Training of District Employees

All employees of the District who have access to social security numbers in the course of performing their duties will be trained to protect the confidentiality of social security numbers. Such training will include instructions on the proper handling of information that contains social security numbers from the time of collection through the destruction of the information.

Distribution of This Policy

The Superintendent or his/her designee will file a written copy of this privacy policy with the Board of Education within 30 days after approval of the policy. The Superintendent or his/her designee will also advise all District employees of the existence of this policy, make a copy of this policy available to each employee, and make this policy available to any member of the public, upon request. If this policy is amended, the Superintendent or his/her designee will file a written copy of the amended policy with the Board of Education, advise District employees of the existence of the amended policy, and make a copy of the amended policy available to each employee.

Treatment of Personally Identifiable Information Under Grant Awards

The Superintendent ensures that the District takes reasonable measures to safeguard: (1) protected personally identifiable information, (2) other information that a federal awarding agency, pass-through agency or State awarding agency designates as sensitive, such as personally identifiable information, 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.

NOTICE OF BREACH

Notification to an individual is required by 815 ILCS 530 et.al. 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 (1) social security number, (2) driver's license number or State identification card number, or (3) financial account information (with any required security codes or passwords), (4) medical information, (5) health insurance information, and/or (6) 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 and 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

PERSONNEL

GENERAL PERSONNEL - IDENTITY PROTECTION

- 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.

LEGAL REF.: Illinois Identity Protection Act, (5 ILCS 179/1 *et seq.*).
Illinois School Student Records Act, (105 ILCS 10/1 *et seq.*)
Personal Information Protection Act, (815 ILCS 530/1 *et seq.*)
Grant Accountability and Transparency Act (30 ILCS 708/)

Adopted: April 14, 2011
Revised: September 26, 2017
Revised: April 23, 2020