Administrative Procedures

Social Security Number Regulations

All covered individuals must safeguard the confidentiality of an individual's Social Security Number ("SSN") by limiting collection, access, or disclosure of a SSN, except where necessary in the ordinary course of business or required by state/federal law or regulation. All covered individuals are prohibited from using all or more than four sequential SSN digits of an employee, student, or other individual in the following circumstances:

(1) Publicly displaying an individual's SSN;
(2) Using a SSN as a primary account number;
(3) Visibly printing a SSN on an identification card, badge, permit or license;
(4) Requiring an individual to use or transmit a SSN over the internet or computer network unless the connection is secure or the transmission is encrypted;
(5) Requiring an individual to use a SSN to gain access to an internet website or computer system or network unless the connection is secure, the transmission is encrypted, or another unique personal identification number is also required to gain access to the computer system or network;
(6) Mailing a document where a SSN is visible without manipulation from the outside of a mailing envelope or package;
(7) Including a SSN in any document or information mailed to a person unless:
   (a) A state/federal law, rule, regulation authorizes, permits or requires inclusion of the SSN;
   (b) The document is part of an application or enrollment process initiated by the individual to whom the document is being mailed;
   (c) The document relates to the individual's health insurance benefits and directly relates to that individual's health insurance contract, policy or employee health insurance benefit;
   (d) The document is a public record mailed in compliance with the Michigan Freedom of Information Act;
   (e) The document or information is a copy of a vital record recorded as provided by law and is mailed to a person entitled to receive that record; or
(f) The document or information is mailed by or at the request of an individual or his/her parent guardian, where the individual’s SSN appears in the document or information.

Exceptions

Covered individuals may use all or more than 4 sequential digits of a SSN under the following circumstances:

(1) A use authorized or required by state or federal statute, rule, or regulation, by court order or rule, or pursuant to legal discovery or process;
(2) Administrative use of a SSN in the ordinary course of business, by an entity or one or its vendors or contractors to:
   (a) Verify an individual's identity related to the individual's employment or do another administrative purpose related to an account, proposed account, transaction, product, service, or employment;
   (b) Verify an individual's claim, credit, criminal, or driving history;
   (c) Detect or deter theft or another crime;
   (d) Lawfully pursue or enforce a person’s legal rights; or
   (e) Provide or administer employee health insurance or retirement benefits or programs.
(3) Continue the use of the social security number as a primary account number, provided that the use began prior to March 1, 2005, and that the use is ongoing, continuous and in the ordinary course of business. Once this use is stopped, it cannot be reinstated.

Storage and Destruction of Documents

All covered individuals shall ensure that any paper or electronic documents or information containing a SSN will be stored and/or disposed of in a secure fashion.

Access to Social Security Numbers

Only those covered individuals with a legitimate business reason shall have access to records or documents containing SSN's. The Human Resources Manager shall determine which personnel have a legitimate reason to access SSN's in the ordinary course of business.
Enforcement

Any covered individual found to have violated this policy or unlawfully disclosed an individual's SSN in violation of the Act will be subject to discipline up to and including discharge. Certain violations of the Act carry criminal and/or civil sanctions. The [School District] will cooperate with appropriate law enforcement or administrative agencies in the apprehension and prosecution of any person who knowingly obtains, uses or discloses SSN's for unlawful purposes.