CONFIDENTIALITY OF PERSONAL IDENTIFYING INFORMATION

Procedure Code: **4705/7825-P**

The following rules govern the collection, use, and disclosure of social security numbers and other personal identifying information.

A. COLLECTION

1. Limitation on Collection and Use of Social Security Numbers

   Social security numbers and other personal identifying information should only be collected when required or authorized by federal or state law. If a unique identifier is needed, then a substitute for the social security number will be used, such as a system-created student identification number that does not use the social security number.

2. Authorized Purposes for Collection

   Social security numbers will be collected only:

   a. for the administration of federal and state income taxes;

   b. for verification of employment eligibility as required by the Immigration Reform and Control Act of 1986;

   c. for Free and Reduced Lunch applications;

   d. if the school system maintained a system of records prior to January 1, 1975, and the disclosure of the social security number was required to verify the identity of an individual;

   e. if it is imperative for the performance of the school system's duties and the need has been plainly documented; or

   f. if the collection and/or use of social security numbers is otherwise authorized by law.

   Prior to the collection of a social security number, the school system department or division that requires the number shall provide an individual, upon request, with a statement of the purpose for which the number will be used. The number will be used only for that stated purpose. In addition, any school system department or division that collects social security numbers shall incorporate such numbers in a student or employee's record in a manner that enables them to be easily redacted upon a valid public records request.

Any school form that requires a social security number must include information on why the number is being collected, what authority the school system is acting upon in collecting the number, and whether the disclosure of the number is mandatory or voluntary.

B. DISCLOSURE

The school system shall not intentionally communicate or make available an individual's social security number or other identifying information to the general public.

1. State Mandated Disclosure Restrictions

   School system officials shall not do any of the following:

   a. intentionally print or imbed a social security number on any card necessary for an individual to gain access to school services;

   b. require an individual to release a social security number on the Internet unless the Internet connection is secure or the social security number is encrypted;

   c. require an individual to use a social security number to gain access to a website, unless access also requires a password or unique PIN;

   d. print an individual's social security number on any materials that are mailed to the individual, unless required by state or federal law; or

   e. print an individual's social security number on a postcard or allow a social security number to be visible through an envelope without the letter being opened.

2. Authorized Disclosures

   School system officials are authorized to disclose social security numbers and other identifying information to an individual or entity outside of the school system in the following circumstances:

   a. pursuant to a court order, warrant, or subpoena;

   b. for public health purposes as required in Chapter 130A of the General Statutes; or

   c. to another governmental entity if necessary for that entity to perform its duties.

3. Public Records

The presence of identifying information in a public record does not change the nature of the public record. If a social security number or personal identifying information is contained within a document subject to release under the Public Records Law, the social security number or personal identifying information will be redacted or removed, and the public record request will be complied with as promptly as possible.

4. Public Display

Social security numbers or personal identifying information must not be placed on identification cards, badges, time cards, employee rosters, bulletin boards, or any other materials or documents widely viewed by others. In addition, documents, materials, or computer screens that display social security numbers or personal identifying information must be kept out of public view at all times.

5. Mailing or Faxing Documents

Documents containing social security numbers or other personal identifying information that must be sent through the mail must not be mailed on a postcard and must be mailed in a manner that does not reveal the number or information through the envelope window or without the envelope being opened.

If a social security number or personal identifying information must be faxed, the fax message must be accompanied by a transmittal sheet that includes a confidentiality notice.

C. ACCESS TO SOCIAL SECURITY NUMBERS OR PERSONAL IDENTIFYING INFORMATION

Only the following individuals within the school system will have access to social security numbers or other personal identifying information:

1. school system personnel, including agents, contractors, and consultants, who require access to perform their jobs or otherwise to render services to the board; and

2. members of the board of education, when access is required to carry out the members' duties and responsibilities.

Under no circumstances may any student have access to social security numbers or personal identifying information for other students or any school system personnel.

D. STORAGE AND DISPOSAL

All documents or files that contain social security numbers or personal identifying information must be stored in a physically secure manner. Social security numbers and

personal identifying information must not be stored on computers or other electronic devices that are not secured against unauthorized access.

Documents or other materials that contain social security numbers or other personal identifying information must not be thrown away through usual trash disposal; they must be discarded or destroyed only in manner that protects their confidentiality, such as shredding.

Any disposal of documents must comply with the *Records Retention and Disposition Schedule for Local Education Agencies*.

E. IMPROPER COLLECTION, DISCLOSURE, OR USE

Any individual who suspects that improper collection, disclosure, or use of a social security number or personal identifying information has occurred shall inform the superintendent or designee.

In the event that a security breach occurs, the affected individual must be notified of the breach. The term "security breach" means an incident of unauthorized access to and acquisition of unencrypted, unredacted records or data containing personal information, when such access (1) results in or is reasonably likely to result in illegal use of the personal information or (2) creates a material risk of harm to the person. In addition, any incident of unauthorized access to and acquisition of *encrypted* records or data containing personal information, along with access to and acquisition of the confidential process or key, will also constitute a security breach. Good faith acquisition of personal information by an employee or agent of the school system for a legitimate business purpose is not considered a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the school system and is not subject to further unauthorized disclosure.

Notice of a security breach must comply with the provisions of G.S. 75-65, including the following.

1. Notice must be provided immediately upon discovery of the breach, unless a law enforcement agency informs school personnel that providing notice may impede a criminal investigation or jeopardize national or homeland security. Any request by a law enforcement agency to delay notice must be in writing; otherwise the school employee receiving the request must document the request in writing at the time it is made. The documentation must include the name and agency of the requesting officer.

2. The notice must be in writing and may also be done via telephone, provided that the phone contact is made directly with the affected person.

3. The notice must be clear and conspicuous.

4. The notice must include a general description of the security breach and a description of the type of information that was subject to the breach.

5. The notice must include action taken by the school system to protect the personal information from further access.

6. The notice must direct the person to remain vigilant by reviewing his or her personal account statements and monitoring his or her credit reports.

7. The notice must include a telephone number that the person may call for further assistance, if such a number exists.

Any individual who fails to comply with legal requirements, board policy, or these regulations will be subject to disciplinary action, up to and including suspension or expulsion for students and termination for employees, and may also be subject to criminal prosecution.

Adopted: March 7, 2016