STATE OF SOUTH CAROLINA
DEPARTMENT OF EDUCATION

Student Unique Numbering System (SUNS) Data Access and Management Policy

July 2023

Contents

I. Introduction

This policy statement pertains to all the data collected and maintained by the South Carolina Department of Education (SCDE) in the Student Unique Numbering System (SUNS). The SUNS database historically has contained data needed to locate the unique identifier of a student who is currently or has previously been enrolled in a South Carolina public school. If a unique identifier does not already exist, the SUNS application will assign one.

The SUNS application is managed by the SCDE in accordance with state and federal laws. The Family Educational Rights and Privacy Act of 1974, as amended (FERPA, 34 CFR Part 99), the Individuals with Disabilities Education Act (IDEA, 34 CFR §§ 300.127 and 300.560-300.576), and South Carolina statutes and policies guard the confidentiality and access to students' educational records. All of these laws and policies are essential to maintaining the confidentiality of student records. This policy statement contains information about the procedures that will be used to follow existing laws and ensure the confidentiality of student records maintained in the SUNS database. It does not expand or in any way change the allowable uses by staff of these systems or the availability of the student records to any other individual.

The SUNS application contains a selected set of data about individual students that will allow for the assignment of a unique student identifier. Historically it has provided a district administrator with the capacity to locate the identifier of a student who has transferred into his/her district from another district within South Carolina. The goal of this system is to maintain a unique identifier for every South Carolina student such that:

1. Only one student is ever assigned a particular number.
2. Once a student is assigned a number, that number is always associated with that student throughout his or her educational career or until he or she leaves the state.
3. A student is only assigned one number so that the student is not duplicated in the SUNS database.

The SUNS application is managed by staff in the SCDE's Division of Data, Technology, and Agency Operations (DTAO), Office of Research, and Data Analysis (ORDA). The Deputy Superintendent of the DTAO is the designated authority to ensure a system of data protection for the SUNS database is maintained in accordance with the FERPA and other relevant state and federal laws and regulations.

II. Guiding Principles

The following principles have been used in establishing a data access and management policy for the SUNS application:

- Student information is a valuable asset of the SCDE and should be treated as such;
- The SCDE manages student information under its control throughout its life cycle, from inception to appropriate destruction;
- The SCDE is responsible for controlling access to and use of student information associated with the SUNS database; and

- The SCDE is responsible for reviewing and updating policies and regulations covering confidential student information and ensuring that its activities comply with state and federal law.

III. Definitions and Background Information Related to this Policy

South Carolina adheres to the confidentiality requirements of both federal and state laws, including but not limited to FERPA, IDEA, the Protection of Pupil Rights Amendment (PPRA), the Health Insurance Portability & Protection Act (HIPPA), and the National School Lunch Act. The following definitions are derived from these laws and other related documents that are relevant to the implementation of the SCDE's Data Access and Management Policy associated with the SUNS application.

- *Privacy* refers to an individual's right to freedom from intrusion due to disclosure of personally identifiable information without consent.
- *Confidentiality* refers to an agency's obligation not to disclose or transmit information about individual students to unauthorized parties. Confidentiality consists of the measures used by an authorized agency to protect how personally identifiable information is collected and maintained and when consent is required to release information.
- *Personally identifiable information* generally includes, but is not limited to:
  - The student's name.
  - The name of the student's parent/guardian.
  - The address of the student or student's family.
  - A personal identifier, such as the state student identifier.
  - Personal characteristics or other information that would make the student's identity easily traceable.

  A small set of this information is essential for assigning identifiers and for identifying students who have transferred from another district within the state or who have returned to the state and already have identifiers. This information will be maintained securely in the SUNS.
- *Disclosure* means to permit access to, revealing, releasing, transferring, or otherwise communicating personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.
- *Access* means to view, print, download, copy, and/or retrieve data from a computer, computer system, or computer network.
- *Confidential data* means information that would tend, by itself or with other information, to identify particular person(s). Confidential data includes information which is intended for the use of a particular person/group and whose unauthorized disclosure could be prejudicial to the individual it identifies.

IV. Protections

To protect the confidentiality of the individual student information and prevent unauthorized disclosure of data, the SCDE has established the following policies and/or practices:

A. Limit Access to the Student Identification/Locator System

District and School Personnel - The superintendent of a public school district (or his or her designee) is responsible for authorizing access to the SUNS application. The superintendent and each authorized staff member must be registered at ed.sc.gov to receive a unique password and login identification. An individual will be granted access to the SUNS application upon signing an assurance statement, having the signed approval of the district superintendent (or his or her designee), and providing the assurance statement to the SCDE. The assurance statement must be on file with the SCDE before the individual will be granted access to the SUNS application. The level of access, building specific or district wide, to the SUNS application will be assigned by the district superintendent (or his or her designee) and managed by the SCDE through the login and password of the user.

District Access through Batch Processing or Individual Student Lookup - The SUNS application will allow districts to upload a batch file of students for their district, download from the identifier system a batch file of students previously submitted from their district, create a student identifier on-line, or use the direct query utility to search for individual students throughout the state. For the purposes of assigning an identifier, districts will not be allowed to view or download batch files uploaded by other districts. District staff may only search for students for the purpose of assigning or locating a unique identifier.

SCDE Staff Access - Only a limited number of SCDE staff have access to the student records stored in the SUNS application. Any SCDE employee or agent assigned responsibilities must sign an assurance statement regarding his or her use and the nondisclosure of confidential information. Examples of staff having access are network administrators, database administrators, and programmers in the ORDA that work directly with districts in implementing and supporting the SUNS database. The level of access to the system, selected districts/buildings or all records, will depend upon the staff member's responsibilities. Other SCDE staff will not have access to the SUNS database.

Early Childhood Partner Agency Personnel - The SCDE is responsible for authorizing access to the SUNS application by their Early Childhood partner agencies. The authorized representative must complete training and receive a certification to receive a unique password and login identification. The training certification must be on file with the SCDE before the individual will be granted access to the SUNS application. The level of access to the SUNS application will be assigned based on the needs of the agency and managed by the SCDE through the login and password of the user.

Other Access - Other individuals, other than those listed above, will not have access to SUNS except under limited circumstances as enumerated below.

B. Access Exceptions

Under this policy, no private or confidential data will be released without the consent of the student or parent except as may be released under the following circumstances as stated in 34 CFR Part 99 Final Regulations for FERPA:

1. To teachers and officials of the district in which the student is enrolled when the determination has been made that there are legitimate educational interests, under Section 99.31(a)(1).

2. To school and district personnel when a student is seeking to enroll, under Section 99.31(a)(2).

3. To comply with a lawfully issued subpoena or court order, under Section 99.31(a)(9)(i). The SCDE shall make a reasonable effort to notify the parent or student, if eighteen or over, of the subpoena or court order.

4. To educational officials in connection with an audit or evaluation of a federal or state supported education program, under Section 99.32(c)(3).

5. To appropriate parties in connection with an emergency if such knowledge is necessary to protect the health and safety of the student or other individuals, under Section 99.36(a). In cases of health or safety emergency, the request for release must first be directed to the school district that owns the data. The Deputy Superintendent, under Section 99.36(a), may also convene a committee to evaluate the request to determine whether the person who would receive the information is in a position to deal with the emergency or not and the extent to which time is of the essence.

6. To researchers whose proposals are approved by the Deputy Superintendent, when a clear legitimate educational interest is established, provided that personally identifiable information if discovered is not disclosed to anyone other than the initiator of the request and the data reporting/database manager. A determination of legitimate educational interest is based in part, on whether sharing information on a specific person would unfavorably affect that individual's ability to learn and function in the classroom. [Section 99.31(a)(6)]

Data will be disclosed only on the conditions that:

1. The party to whom the data are released does not disclose the information to any third party without the prior written consent of the Deputy Superintendent, the company who provided the student assessment data (if assessment data are being disclosed), or the school district that owns the data;

2. The data are protected in a manner that does not permit the personal

identification of an individual by anyone except the party referenced in the disclosure; and

3. The data are destroyed when no longer needed for the purposes under which the disclosure was granted.

The Deputy Superintendent of the DTAO will account to the State Superintendent of Education for all disclosures or requests for disclosures. This includes keeping a list of the data, nature, and purposes of the disclosure, and to whom the disclosure was made.

C. System Security

The SUNS database will be maintained in a secure environment under the control of the SCDE. The Office of the Chief Information Officer (CIO) administrator and staff will monitor security notices affecting the system software and will maintain the current software patches for the system components housed at the SCDE. The Chief Information Security Office (CISO) will monitor the access logs for the database for activity in violation of this Data Access and Management Policy.

A web-based application used by district personnel to access or generate a child's identifier and to perform near-match resolution is located at the SCDE. The SUNS application also allows for internet-based batch submission of student records for retrieval or generation of an identifier. The CIO staff works closely with CISO staff to ensure appropriate firewall protection and intrusion detection efforts are in place for the system components housed at the SCDE. The CIO and CISO staff will monitor security notices affecting the system software and will work to ensure that the current software patches are in place for the system components located at the SCDE.

V. Data Use and Release

A. Agency Data Sharing

Currently, the SCDE does not grant access to the statewide SUNS to other state agencies. The SCDE has inter-agency agreements to share limited amounts of data for the benefit of the children of South Carolina that are allowed by law. Other sharing of student data will be prohibited. The SCDE will comply with requests for individual student data from federal governmental agencies as required by law.

B. Parents

Upon the request of any individual (or the individual's parent/guardian if the individual is under the age of eighteen) under Section 99.20 of the FERPA to gain access to his/her (child's) record contained in the SUNS, the Deputy Superintendent of the DTAO will provide a copy of all or any portion in a comprehensible form. Since the data actually belong to the local educational agencies or Early Childhood Partner Agencies, parents/guardians should seek first to review and amend the student's record through the relevant agency owner.

Under S.C. Code Ann. § 20-7-100, "Each parent, whether the custodial or non-custodial parent of the child, has equal access and the same right to obtain all educational records and medical records of their minor children and the right to participate in their children's school activities unless prohibited by order of the court." To the extent possible, SCDE staff will contact the school of record for a child to determine whether there is a court order preventing the release of information to a non-custodial parent.

VI. Improper Disclosure of Student Records

The Deputy Superintendent of the DTAO has the responsibility for determining whether a request for access to the student records constitutes a legitimate request for an appropriate usage of student data. If the request does not meet standards established by the SCDE for the lawful release of student data, then the request will be denied.

The Deputy Superintendent of the DTAO is also responsible for determining if personally identifiable information has been inappropriately disclosed by the SCDE, school district, partner agency official, or a third party allowed use of the data in violation of this policy. If the disclosure is made by the SCDE, school district, or partner agency official in violation of federal law, the official may be subject to a personnel action, including termination (if a SCDE employee), or suspension of login privileges. If an improper disclosure is made by someone other than the SCDE, school district, or partner agency official, then the parties will not have access to any data reporting/database information for five years as required by the FERPA. In addition, all violations will be reported to the appropriate federal and state enforcement agencies.

VII. Ownership of the Data

School districts or other primary sources of the data, such as Early Childhood Partner Agencies, that are located in the SUNS are the originators and owners of those data. The Deputy Superintendent of the DTAO functions as the custodian of the data in the SCDE. To protect the data in its custody, the SCDE has established this policy, which is implemented by the Deputy Superintendent of the DTAO. The policy ensures that all data are securely maintained with safeguards on all personally identifiable information in the databases.

SUNS Application District Assurance Statement

Individual student information contained in the South Carolina Department of Education's (SCDE) Student Unique Numbering System (SUNS) is collected for the purpose of generating unique student identification numbers. The data are protected by state and federal laws and must be maintained in a confidential manner at all times. As an employee of a local school district or the SCDE that has access to records in the SUNS, you are required to maintain this information in a confidential manner. The unauthorized access to, modification, deletion, or disclosure of information from the SUNS may compromise the integrity of the system, violate individual student rights of privacy, and/or constitute a punishable act and subject the employer to a loss of federal funds.

Unauthorized viewing, reproduction/copying, and/or distribution of any student record or information outside the intended and approved use of the SUNS are strictly prohibited. Users violating the authorized use of the SUNS will lose access privileges to the system. Illegal access or misuse of this information may also be cause for disciplinary action, including termination.

I have received and read the SCDE's Data Access and Management Policy Statement for the SCDE's SUNS application.

I acknowledge and agree to the above requirements.

District/Organization Name: _____

Employee Name: _____

Employee Signature: _____

Employee Phone Number_____

Date: _____

District Superintendent or Designee Signature: _____

Date: _____

SAMPLE SUNS System Early Childhood Partner Training Certification

Individual student information contained in the South Carolina Department of Education's (SCDE) Student Unique Numbering System (SUNS) is collected for the purpose of generating unique student identification numbers. The data are protected by state and federal laws and must be maintained in a confidential manner at all times. As an employee of a SCDE Early Childhood Partner Agency with access to records in the SUNS, you are required to maintain this information in a confidential manner. The unauthorized access to, modification, deletion, or disclosure of information from the SUNS system may compromise the integrity of the system, violate individual student rights of privacy, and/or constitute a punishable act and subject the partnering agency to loss of access to the SUNS system.

Unauthorized viewing, reproduction/copying, and/or distribution of any student record or information outside the intended and approved use of the SUNS are strictly prohibited. Users violating the authorized use of the SUNS will lose access privileges to the system. Illegal access or misuse of this information may result in access to the SUNS being revoked.

I have received and read the SCDE's SUNS User Guide – ID Assignment Process and I certify that I have completed the required hours of SUNS training.

I acknowledge and agree to the above requirements.

Partner Agency Name: _____

Facility Name: _____

Employee Name: _____

Employee Signature: _____

Employee Phone Number: _____

Date: _____

SCDE Representative Signature: _____
Insert trainer name here

Date: _____